Referencia de autorizaciones de servicio

Referencia de autorizaciones de servicio

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

Referencia de autorizaciones de servicio: Referencia de autorizaciones de servicio

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Referencia 1
Acciones, recursos y claves de condición 1
Tabla Acciones 1
Tabla Tipos de recurso 2
Tabla Claves de condición 3
AWS Administración de cuentas 19
AWS Activa 26
Amazon AI Operations 29
Alexa for Business 41
AmazonMediaImport 60
AWS Amplify 63
AWS Amplify Admin 72
AWS Amplify UI Builder 81
Apache Kafka APIs para clústeres de Amazon MSK 94
Amazon API Gateway 102
AWS App Mesh 105
AWS Vista previa de App Mesh 117
AWS App Runner 125
AWS App Studio 141
AWS App2Container 145
AWS AppConfig 147
AWS AppFabric 164
Amazon AppFlow 174
Amazon AppIntegrations 182
AWS Application Auto Scaling 199
AWS Servicio de generación de perfiles de costes de aplicaciones 208
Application Discovery Arsenal 211
AWS Application Discovery Service 214
AWS Servicio de migración de aplicaciones 227
Controlador de recuperación de aplicaciones de Amazon: Cambio de zona 299
AWS Servicio de transformación de aplicaciones 310
Amazon AppStream 2.0 314
AWS AppSync 339
AWS Artefacto 356

Amazon Athena 362
AWS Audit Manager 378
Amazon Aurora DSQL 392
AWS Auto Scaling 399
AWS Intercambio de datos B2B 402
AWS Backup 409
AWS Backup Gateway 433
AWS Búsqueda de Backup 440
AWS Almacenamiento de Backup 445
AWS Batch 449
Amazon Bedrock 465
AWS Billing 515
AWS Billing Y exportaciones de datos de gestión de costes 523
AWS Billing Y calculadora de precios de gestión de costos 528
AWS Billing Conductor 537
AWS Billing Consola 546
Amazon Braket 550
AWS Servicio presupuestario 556
AWS BugBust 562
AWS Certificate Manager 570
AWS Chatbot 577
Amazon Chime 586
AWS Salas limpias 653
AWS Salas limpias (ML) 687
Nube de AWS API de control 712
Amazon Cloud Directory 715
Nube de AWS Mapa 729
AWS Cloud9 738
AWS CloudFormation 747
Amazon CloudFront 775
Amazon CloudFront KeyValueStore 804
AWS ClouDHSM 807
Amazon CloudSearch 815
AWS CloudShell 822
AWS CloudTrail 826
AWS CloudTrail Datos 847

Amazon CloudWatch 850
Información sobre CloudWatch aplicaciones de Amazon 865
Señales CloudWatch de aplicaciones de Amazon 871
Amazon, CloudWatch evidentemente 877
Amazon CloudWatch Internet Monitor 886
Amazon CloudWatch Logs 891
Monitor sintético CloudWatch de Amazon Network 913
Administrador de acceso a Amazon CloudWatch Observability 918
Servicio de administración de Amazon CloudWatch Observability 924
AWS CloudWatch RON 927
Amazon CloudWatch Synthetics 933
AWS CodeArtifact 942
Amazon CodeCatalyst 952
AWS CodeCommit 963
AWS CodeConnections 984
AWS CodeDeploy 999
AWS CodeDeploy servicio de comandos de host seguro 1012
Amazon CodeGuru 1015
Amazon CodeGuru Profiler 1017
CodeGuru Revisor de Amazon 1023
CodeGuru Seguridad de Amazon 1031
AWS CodePipeline 1036
AWS CodeStar 1047
AWS CodeStar Conexiones 1055
AWS CodeStar Notificaciones 1070
Amazon CodeWhisperer 1079
Amazon Cognito Identity 1086
Amazon Cognito Sync 1094
Grupos de usuarios de Amazon Cognito 1100
Amazon Comprehend 1119
Amazon Comprehend Medical 1157
AWS Compute Optimizer 1164
AWS Config 1175
Amazon Connect Cases 1203
Amazon Connect Customer Profiles 1213
Campañas externas de Amazon Connect 1232

Amazon Connect Voice ID 1240
AWS Servicio de conectores 1247
AWS Management Console Aplicación móvil 1250
AWS Facturación consolidada 1252
AWS Catálogo de controles 1255
AWS Torre de Control 1258
AWS Informe de costo y uso 1272
AWS Servicio Cost Explorer 1277
AWS Centro de optimización de costes 1292
AWS Servicio de verificación de clientes 1295
AWS Data Exchange 1298
Amazon Data Lifecycle Manager 1309
AWS Data Pipeline 1313
AWS Database Migration Service 1324
Database Query Metadata Service 1358
AWS DataSync 1361
Amazon DataZone 1377
AWS Deadline Cloud 1404
AWS DeepComposer 1442
AWS DeepRacer 1449
Amazon Detective 1472
AWS Device Farm 1482
El DevOps gurú de Amazon 1502
AWS Herramientas de diagnóstico 1509
AWS Direct Connect 1514
AWS Directory Service 1531
AWS Datos de Directory Service 1555
Amazon DocumentDB Elastic Clusters 1566
Amazon DynamoDB 1588
Amazon DynamoDB Accelerator (DAX) 1613
Amazon EC2 Auto Scaling 1621
Amazon EC2 Image Builder 1650
Amazon EC2 Instance Connect 1684
Amazon EKS Auth 1689
AWS Elastic Beanstalk 1692
Amazon Elastic Block Store (EBS) 1713

Amazon Elastic Container Registry 1718
Amazon Elastic Container Registry Public 1731
Amazon Elastic Container Service 1738
AWS Elastic Disaster Recovery 1772
Amazon Elastic File System 1807
Amazon Elastic Kubernetes Service 1820
AWS Elastic Load Balancing 1842
AWS Elastic Load Balancing V2 1860
Amazon Elastic MapReduce 1893
Amazon Elastic Transcoder 1913
Amazon Elastic VMware Service 1918
Amazon ElastiCache 1923
AWS Dispositivos y software elementales 1984
AWS Servicio de activación de software y dispositivos Elemental 1988
AWS Elemental MediaConnect 1993
AWS Elemental MediaConvert 2002
AWS Elemental MediaLive 2013
AWS Elemental MediaPackage 2041
AWS Elemental MediaPackage V2 2048
AWS VOD elemental MediaPackage 2060
AWS Elemental MediaStore 2066
AWS Elemental MediaTailor 2073
AWS Fundas Elemental Support 2085
AWS Contenido de Elemental Support 2091
Amazon EMR en EKS (Contenedores de EMR) 2093
Amazon EMR Serverless 2101
AWS Mensajería de voz y SMS para el usuario final V2 2107
AWS Mensajería para usuarios finales en redes sociales 2129
AWS Resolución de entidades 2135
Amazon EventBridge 2144
Amazon EventBridge Pipes 2163
Amazon EventBridge Scheduler 2168
EventBridge Esquemas de Amazon 2174
AWS Servicio de inyección de errores 2183
Amazon FinSpace 2193
FinSpace API de Amazon 2208

AWS Firewall Manager 2211
Amazon Forecast 2223
Amazon Fraud Detector 2245
AWS Nivel gratuito 2276
Amazon FreeRTOS 2278
Amazon FSx 2285
GameLift Servidores Amazon 2307
Amazon GameLift Streams 2338
AWS Acelerador global 2344
AWS Glue 2357
AWS Glue DataBrew 2414
AWS Ground Station 2424
GroundTruth Etiquetado de Amazon 2434
Amazon GuardDuty 2439
AWS Salud APIs y notificaciones 2455
AWS HealthImaging 2461
AWS HealthLake 2468
AWS HealthOmics 2475
Amazon Honeycode 2496
AWS Analizador de acceso IAM 2503
AWS Centro de identidad de IAM 2511
AWS Directorio del Centro de Identidad de IAM 2538
AWS IAM Identity Center (servicio OIDC) 2551
AWS Identity and Access Management (IAM) 2554
AWS Funciones de Identity and Access Management en cualquier lugar 2594
AWS Almacén de identidades 2601
AWS Autenticación del almacén de identidades 2608
AWS Sincronización de identidades 2610
AWS Servicio de importación y exportación de discos 2615
Amazon Inspector 2619
Amazon Inspector2 2628
Amazon InspectorScan 2642
Amazon Interactive Video Service 2645
Amazon Interactive Video Service Chat 2665
AWS Servicio de facturación 2671
AWS IoT 1-Click 2677

AWS IoT Analytics 2683
AWS Asesor de dispositivos básicos de IoT 2691
AWS Probador de dispositivos IoT 2697
AWS Eventos de IoT 2700
AWS IoT Fleet Hub para la gestión de dispositivos 2709
AWS IoT FleetWise 2713
AWS IoT Greengrass 2729
AWS IoT Greengrass V2 2752
AWS Empleos de IoT DataPlane 2765
AWS Integraciones gestionadas de IoT 2768
AWS IoT SiteWise 2784
AWS IoT TwinMaker 2803
AWS IoT Wireless 2815
AWS IQ 2840
AWS Permisos IQ 2850
Amazon Kendra 2854
Amazon Kendra Intelligent Ranking 2870
Amazon Keyspaces (for Apache Cassandra) 2874
Amazon Kinesis Analytics 2882
Amazon Kinesis Analytics V2 2887
Amazon Kinesis Data Streams 2895
Amazon Kinesis Firehose 2906
Amazon Kinesis Video Streams 2910
AWS Lake Formation 2921
AWS Lambda 2932
AWS Launch Wizard 2951
Amazon Lex 2959
Amazon Lex V2 2969
AWS License Manager 2994
AWS License Manager Administrador de suscripciones de Linux 3005
AWS Suscripciones de usuarios de License Manager 3010
Amazon Lightsail 3017
Amazon Location 3054
Amazon Location Service Maps 3068
Amazon Location Service Places 3071
Amazon Location Service Routes 3074

Amazon Lookout for Equipment 3077
Amazon Lookout for Metrics 3090
Amazon Lookout for Vision 3098
Amazon Machine Learning 3105
Amazon Macie 3112
AWS Pruebas de aplicaciones de modernización de mainframes 3131
AWS Servicio de modernización de mainframe 3141
Amazon Managed Blockchain 3153
Amazon Managed Blockchain Query 3163
Amazon Managed Grafana 3166
Amazon Managed Service for Prometheus 3175
Amazon Managed Streaming for Apache Kafka 3190
Amazon Managed Streaming for Kafka Connect 3208
Amazon Managed Workflows for Apache Airflow 3217
AWS Marketplace 3223
AWS Marketplace Catálogo 3230
AWS Marketplace Servicio de análisis de comercio 3236
AWS Marketplace Servicio de despliegue 3238
AWS Marketplace Descubrimiento 3243
AWS Marketplace Servicio de asignación de derechos 3245
AWS Marketplace Servicio de creación de imágenes 3248
AWS Marketplace Portal de administración 3250
AWS Marketplace Servicio de medición 3255
AWS Marketplace Marketplace privado 3258
AWS Marketplace Integración de sistemas de aprovisionamiento 3262
AWS Marketplace Informes 3265
AWS Marketplace Informes del vendedor 3268
AWS Marketplace Información sobre los proveedores 3270
Amazon Mechanical Turk 3279
Amazon MemoryDB 3288
Servicio de entrega de mensajes de Amazon 3312
Amazon Message Gateway Service 3315
AWS Microservice Extractor para .NET 3319
AWS Créditos del Migration Acceleration Program 3321
AWS Migration Hub 3324
AWS Organizador de Migration Hub 3334

AWS Migration Hub Refactoriza los espacios 3342
AWS Recomendaciones de estrategia de Migration Hub 3362
Amazon Mobile Analytics 3368
Amazon Monitron 3371
Amazon MQ 3382
Aprobación multipartita 3391
Amazon Neptune 3400
Analítica de Amazon Neptune 3407
AWS Network Firewall 3423
Network Flow Monitor 3439
AWS Administrador de red 3447
AWS Chat de Network Manager 3471
Amazon Nimble Studio 3475
Amazon One Enterprise 3495
Amazon OpenSearch 3505
OpenSearch Ingestión de Amazon 3508
Amazon OpenSearch Serverless 3515
OpenSearch Servicio Amazon 3524
AWS OpsWorks 3549
AWS OpsWorks Administración de la configuración 3561
AWS Organizations 3566
AWS Outposts 3582
AWS Panorama 3590
AWS Servicio de computación paralela 3599
AWS Administración de cuentas de Partner Central 3612
AWS Partner Central Selling 3615
AWS Criptografía de pagos 3630
AWS Pagos 3641
AWS Performance Insights 3648
Amazon Personalize 3654
Amazon Pinpoint 3667
Servicio de correo electrónico de Amazon Pinpoint 3697
Servicio de SMS y voz de Amazon Pinpoint 3713
Amazon Polly 3717
AWS Lista de precios 3720
AWS Conector CA privado para Active Directory 3723

AWS Conector CA privado para SCEP 3732
AWS Autoridad de certificación privada 3737
AWS PrivateLink 3745
AWS Proton 3747
AWS Consola de órdenes de compra 3777
Amazon Q 3783
Amazon Q Business 3796
Aplicaciones de Amazon Q Business Q 3819
Amazon Q Developer 3836
Amazon Q in Connect 3840
Amazon QLDB 3863
Amazon QuickSight 3872
API de datos de Amazon RDS 3919
Autenticación IAM de Amazon RDS 3924
AWS Papelera de reciclaje 3927
Amazon Redshift 3933
API de datos de Amazon Redshift 3979
Amazon Redshift sin servidor 3985
Amazon Rekognition 4004
AWS RePost Private 4021
AWS Centro de resiliencia 4025
AWS Resource Access Manager (RAM) 4044
AWS Explorador de recursos 4063
API de etiquetado de grupos de recursos de Amazon 4071
AWS Resource Groups 4075
Amazon RHEL Knowledgebase Portal 4083
AWS RoboMaker 4085
Amazon Route 53 4100
Amazon Route 53 Dominios 4117
Perfiles de Amazon Route 53 4125
Amazon Route 53 Recovery Cluster 4132
Amazon Route 53 Recovery Controls 4135
Amazon Route 53 Recovery Readiness 4143
Amazon Route 53 Resolver 4151
Amazon S3 Express 4175
Amazon S3 Glacier 4210

Amazon S3 Object Lambda 4218
Amazon S3 en Outposts 4245
Tablas de Amazon S3 4314
Asistente de ciencia SageMaker de datos de Amazon 4324
Capacidades SageMaker geoespaciales de Amazon 4326
Amazon SageMaker con MLflow 4335
AWS Savings Plans 4344
AWS Secrets Manager 4349
AWS Security Hub 4376
AWS Respuesta a incidentes de seguridad 4404
Amazon Security Lake 4410
AWS Servicio de migración de servidores 4442
AWS Serverless Application Repository 4449
AWS Servicio: Oracle Database@AWS 4454
AWS Service Catalog 4470
AWS servicio que proporciona redes privadas gestionadas 4498
Service Quotas 4506
Amazon SES 4515
AWS Shield 4534
AWS Firmante 4545
AWS Inicio de sesión 4552
Acciones, recursos y claves de condición para Amazon Simple Email Service - Administrador de correo electrónico 4555
Amazon Simple Email Service v2 4573
Amazon Simple Workflow Service 4604
Amazon SimpleDB 4623
AWS SimSpace Weaver 4627
AWS Mostrar administración de dispositivos 4632
AWS Snowball 4637
Amazon SNS 4644
AWS SQL Workbench 4655
Amazon SQS 4672
AWS Step Functions 4678
AWS Storage Gateway 4689
AWS Cadena de suministro 4714
AWS Support 4723

AWS Support Aplicación en Slack 4730
AWS Support Consola 4735
AWS Support Planes 4738
AWS Support Recomendaciones 4741
AWS Sostenibilidad 4743
AWS Systems Manager 4746
AWS Systems Manager para SAP 4791
AWS System Manager GUI Connect 4799
AWS Gestor de Sistemas Gestor de Incidentes 4802
AWS Contactos del administrador de incidentes de Systems Manager 4811
AWS Configuración rápida de Systems Manager 4820
Editor de etiquetas 4825
AWS Configuración fiscal 4828
AWS Creador de redes de telecomunicaciones 4832
Amazon Textract 4843
Amazon Timestream 4851
Amazon Timestream InfluxDB 4862
AWS Tiros 4869
Amazon Transcribe 4872
AWS Transfer Family 4887
AWS Transformación 4901
Amazon Translate 4904
AWS Trusted Advisor 4910
AWS Notificaciones de usuario 4921
AWS Notificaciones de usuario y contactos 4930
AWS Suscripciones de usuarios 4935
AWS Acceso verificado 4938
Amazon Verified Permissions 4940
Amazon VPC Lattice 4949
Amazon VPC Lattice Services 4980
AWS WAF 4987
AWS WAF Regional 5001
AWS WAF V2 5016
AWS Herramienta Well-Architected 5038
AWS Mimbre 5056
Amazon WorkDocs 5060

Amazon WorkLink 5072
Amazon WorkMail 5080
Flujo de WorkMail mensajes de Amazon 5103
Amazon WorkSpaces 5106
Gestor WorkSpaces de aplicaciones de Amazon 5125
AWS WorkSpaces Instancias gestionadas 5128
Navegador Amazon WorkSpaces Secure 5133
Amazon WorkSpaces Thin Client 5150
AWS X-Ray 5158
Recursos relacionados 5170
Acceso mediante programación a información de referencia del servicio 5171
Definiciones de campos adicionales 5174
..... 5177

Referencia

La referencia de autorización de servicio proporciona una lista de las acciones, los recursos y las claves de condición que admite cada AWS servicio. Puede especificar las acciones, los recursos y las claves de condición en las políticas AWS Identity and Access Management (IAM) para administrar el acceso a AWS los recursos.

Contenido

- Claves de condiciones, recursos y acciones de los servicios AWS
- Recursos relacionados

Claves de condiciones, recursos y acciones de los servicios AWS

Cada AWS servicio puede definir acciones, recursos y claves de contexto de condiciones para su uso en las políticas de IAM. En este tema se describe cómo se documentan los elementos proporcionados para cada servicio.

Cada tema se compone de tablas que proporcionan la lista de las acciones, los recursos y las claves de condición disponibles.

Tabla Acciones

La tabla Actions (Acciones) muestra todas las acciones que puede utilizar en un elemento `Action` de la declaración de política de IAM. No todas las operaciones de API que se definen mediante un servicio se pueden utilizar como una acción en una política de IAM. Algunos servicios incluyen acciones exclusivas que no corresponden directamente con una operación de la API. Estas acciones se indican con [permission only] ([solo permiso]). Utilice esta lista para determinar qué acciones se pueden utilizar en una política de IAM. Para obtener más información sobre los elementos `Action`, `Resource` o `Condition`, consulte Referencia de los elementos de las políticas JSON de IAM. Las columnas Actions (Acciones) y Description (Descripción) de la tabla son descriptivas.

- La columna Access level (Nivel de acceso) describe cómo se clasifica la acción (Lista, lectura, escritura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte Descripción de los resúmenes de nivel de acceso en los resúmenes de políticas.

- La columna Resource types (Tipos de recurso) indica si la acción admite permisos de nivel de recursos. Si la columna está vacía, la acción no admite permisos de nivel de recursos y debe especificar todos los recursos ("*") en su política. Si la columna incluye un tipo de recurso, puede especificar el ARN del recurso en el elemento `Resource` de la política. Para obtener más información acerca de dicho recurso, consulte esa fila en la tabla Resource types (Tipos de recurso). Todas las acciones y los recursos que se incluyen en una declaración deben ser compatibles entre sí. Si especifica un recurso que no es válido para la acción, cualquier solicitud de uso de dicha acción dará error y el `Effect` de la declaración no se aplica.

  Los recursos necesarios se indican en la tabla con un asterisco (*). Si especifica un ARN de permiso de recursos en una instrucción mediante esta acción, deberá ser de este tipo. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno pero no el otro.
- La columna Condition keys (Claves de condición) incluye claves que puede especificar en el elemento `Condition` de una instrucción de política. Las claves de condición pueden ser compatibles con una acción o con una acción y un recurso específico. Preste especial atención a si la clave está en la misma fila que un tipo de recurso específico. Esta tabla no incluye las claves de condición globales que están disponibles para cualquier acción o en circunstancias no relacionadas. Para obtener más información sobre las claves de condición globales, consulte Claves de contexto de condición globales de AWS.
- La columna Acciones dependientes incluye permisos adicionales que debería tener, además del permiso para la acción en sí, para llamar correctamente a la acción. Esto puede ser necesario si la acción obtiene acceso a más de un recurso.

  No se requieren acciones dependientes en todos los escenarios. Consulta la documentación del servicio individual para obtener más información sobre cómo proporcionar permisos detallados a los usuarios.

Tabla Tipos de recurso

La tabla Resource types (Tipos de recurso) muestra todos los tipos de recursos que puede especificar como ARN en el elemento de política `Resource`. No todos los tipos de recursos se pueden especificar con cada acción. Algunos tipos de recursos funcionan solo con determinadas acciones. Si especifica un tipo de recurso en una instrucción con una acción que no admite ese tipo de recurso, la instrucción no permite el acceso. Para obtener más información sobre el elemento `Resource`, consulte Elementos de las políticas JSON de IAM: Recourse.

- La columna ARN especifica el formato de nombre de recurso de Amazon (ARN) que debe utilizar para hacer referencia a los recursos de este tipo. Las partes precedidas por $ deben sustituirse por los valores reales de su escenario. Por ejemplo, si se observa `$user-name` en un ARN, se debe reemplazar esa cadena con el nombre de usuario real o una variable de política que contenga un nombre de usuario. Para obtener más información al respecto ARNs, consulte ARNsIAM.
- La columna Condition keys (Claves de condición) especifica las claves de contexto de condiciones que puede incluir en una instrucción de política de IAM solo cuando se incluyen en la instrucción este recurso y una acción de apoyo de la tabla anterior.

Tabla Claves de condición

La tabla Condition keys (Claves de condición) muestra todas las claves de contexto de condiciones que puede utilizar en un elemento `Condition` de una instrucción de política de IAM. No todas las claves se pueden especificar con cada acción o recurso. Algunas solo funcionan con determinados tipos de acciones y recursos. Para obtener más información sobre el elemento `Condition`, consulte Elementos de las políticas JSON de IAM: Condition.

- La columna Type (Tipo) especifica el tipo de datos de la clave de condición. Este tipo de datos determina qué operadores de condición puede usar para comparar los valores de la solicitud con los valores de la instrucción de política. Debe utilizar un operador que sea adecuado para el tipo de datos. Si utiliza un operador incorrecto, no habrá coincidencias y la declaración de política no se aplica.

  Si la columna Type (Tipo) especifica una "Lista de..." uno de los tipos simples, puede usar varias claves y valores en sus políticas. Para ello, utilice prefijos de conjunto de condiciones con los operadores. Utilice el prefijo `ForAllValues` para especificar que todos los valores de la solicitud deben coincidir con un valor de la instrucción de política. Utilice el prefijo `ForAnyValue` para especificar que al menos un valor de la solicitud debe coincidir con uno de los valores de la instrucción de política.

Temas

- Claves de condición, acciones y recursos para AWS Account Management
- Acciones, recursos y claves de condición para AWS Activate
- Claves de condiciones, recursos y acciones para Amazon AI Operations
- Acciones, recursos y claves de condición para Alexa for Business

- Acciones, recursos y claves de condición para AmazonMediaImport
- Acciones, recursos y claves de condición para AWS Amplify
- Acciones, recursos y claves de condición para AWS Amplify Admin
- Acciones, recursos y claves de condición para AWS Amplify UI Builder
- Claves de condición, recursos y acciones para clústeres de Apache Kafka APIs para Amazon MSK
- Acciones, recursos y claves de condición de Amazon API Gateway
- Acciones, recursos y claves de condición para AWS App Mesh
- Acciones, recursos y claves de condición para AWS App Mesh Preview
- Acciones, recursos y claves de condición para AWS App Runner
- Acciones, recursos y claves de condición para AWS App Studio
- Acciones, recursos y claves de condición de AWS App2Container
- Acciones, recursos y claves de condición para AWS AppConfig
- Acciones, recursos y claves de condición para AWS AppFabric
- Acciones, recursos y claves de condición de Amazon AppFlow
- Acciones, recursos y claves de condición de Amazon AppIntegrations
- Acciones, recursos y claves de condición para AWS Application Auto Scaling
- Acciones, recursos y claves de condición para el servicio AWS Application Cost Profiler
- Acciones, recursos y claves de condición para Application Discovery Arsenal
- Acciones, recursos y claves de condición para AWS Application Discovery Service
- Acciones, recursos y claves de condición para AWS Application Migration Service
- Acciones, recursos y claves de condición de Amazon Application Recovery Controller - Zonal Shift
- Acciones, recursos y claves de condición para AWS Application Transformation Service
- Acciones, recursos y claves de condición de Amazon AppStream 2.0
- Acciones, recursos y claves de condición para AWS AppSync
- Acciones, recursos y claves de condición para AWS Artifact
- Acciones, recursos y claves de condición para Amazon Athena
- Acciones, recursos y claves de condición para AWS Audit Manager
- Claves de condición, recursos y acciones de Amazon Aurora DSQL
- Acciones, recursos y claves de condición para AWS Auto Scaling

- Acciones, recursos y claves de condición para el intercambio de datos B2B de AWS
- Acciones, recursos y claves de condición para AWS Backup
- Acciones, recursos y claves de condición para AWS Backup Gateway.
- Acciones, recursos y claves de condición de AWS Backup Search
- Acciones, recursos y claves de condición para el almacenamiento de AWS Backup
- Acciones, recursos y claves de condición para AWS Batch
- Acciones, recursos y claves de condición para Amazon Bedrock
- Acciones, recursos y claves de condición para AWS Billing
- Acciones, recursos y claves de condición para exportaciones de datos de AWS Billing y gestión de costos
- Claves de acciones, recursos y condiciones de la calculadora de precios de AWS Billing And Cost Management
- Acciones, recursos y claves de condición para AWS Billing Conductor
- Acciones, recursos y claves de condición para AWS Billing Console
- Acciones, recursos y claves de condición para Amazon Braket
- Acciones, recursos y claves de condición para AWS Budget Service
- Acciones, recursos y claves de condición para AWS BugBust
- Acciones, recursos y claves de condición para AWS Certificate Manager
- Acciones, recursos y claves de condición para AWS Chatbot
- Acciones, recursos y claves de condición para Amazon Chime
- Acciones, recursos y claves de condición para AWS Clean Rooms
- Acciones, recursos y claves de condición para AWS Clean Rooms ML
- Claves de condición, acciones y recursos para la API de Nube de AWS Control
- Acciones, recursos y claves de condición para Amazon Cloud Directory
- Acciones, recursos y claves de condición para Nube de AWS Map
- Acciones, recursos y claves de condición para AWS Cloud9
- Acciones, recursos y claves de condición para AWS CloudFormation
- Acciones, recursos y claves de condición de Amazon CloudFront
- Acciones, recursos y claves de condición de Amazon CloudFront KeyValueStore

- Acciones, recursos y claves de condición para AWS CloudHSM
- Acciones, recursos y claves de condición de Amazon CloudSearch
- Acciones, recursos y claves de condición para AWS CloudShell
- Acciones, recursos y claves de condición para AWS CloudTrail
- Claves de condición, recursos y acciones de los AWS CloudTrail datos
- Acciones, recursos y claves de condición de Amazon CloudWatch
- Acciones, recursos y claves de condición de Amazon CloudWatch Application Insights
- Claves de condición, recursos y acciones de Amazon CloudWatch Application Signals
- Acciones, recursos y claves de condición de Amazon CloudWatch Evidently
- Claves de condición, recursos y acciones de Amazon CloudWatch Internet Monitor
- Claves de condición, recursos y acciones de Amazon CloudWatch Logs
- Claves de condición, recursos y acciones de Amazon CloudWatch Network Synthetic Monitor
- Claves de condición, recursos y acciones de Amazon CloudWatch Observability Access Manager
- Acciones, recursos y claves de condición del Servicio de administración de Amazon CloudWatch Observability
- Claves de condición, recursos y acciones de AWS CloudWatch RUM
- Acciones, recursos y claves de condición de Amazon CloudWatch Synthetics
- Acciones, recursos y claves de condición para AWS CodeArtifact
- Acciones, recursos y claves de condición de Amazon CodeCatalyst
- Acciones, recursos y claves de condición para AWS CodeCommit
- Acciones, recursos y claves de condición para AWS CodeConnections
- Acciones, recursos y claves de condición para AWS CodeDeploy
- Claves de condición, recursos y acciones para el servicio de comandos de host AWS CodeDeploy seguro
- Acciones, recursos y claves de condición de Amazon CodeGuru
- Claves de condición, recursos y acciones de Amazon CodeGuru Profiler
- Acciones, recursos y claves de condición de Amazon CodeGuru Reviewer
- Claves de condición, recursos y acciones de Amazon CodeGuru Security
- Acciones, recursos y claves de condición para AWS CodePipeline

- Acciones, recursos y claves de condición para AWS CodeStar
- Claves de condición, recursos y acciones de AWS CodeStar Connections
- Claves de condición, recursos y acciones de las AWS CodeStar notificaciones
- Acciones, recursos y claves de condición de Amazon CodeWhisperer
- Acciones, recursos y claves de condición para Amazon Cognito Identity
- Acciones, recursos y claves de condición para Amazon Cognito Sync
- Acciones, recursos y claves de condición para los grupos de usuarios de Amazon Cognito
- Acciones, recursos y claves de condición para Amazon Comprehend
- Acciones, recursos y claves de condición para Amazon Comprehend Medical
- Acciones, recursos y claves de condición para AWS Compute Optimizer
- Acciones, recursos y claves de condición para AWS Config
- Acciones, recursos y claves de condición para Amazon Connect Cases
- Acciones, recursos y claves de condición para Amazon Connect Customer Profiles
- Acciones, recursos y claves de condición de las campañas salientes de Amazon Connect
- Acciones, recursos y claves de condición para Amazon Connect Voice ID
- Acciones, recursos y claves de condición para AWS Connector Service
- Acciones, recursos y claves de condición para Aplicación móvil de AWS Management Console
- Acciones, recursos y claves de condición para la facturación consolidada de AWS
- Acciones, recursos y claves de condición para AWS Control Catalog
- Acciones, recursos y claves de condición para AWS Control Tower
- Claves de condición, recursos y acciones para los Informes de costos y usos de AWS
- Acciones, recursos y claves de condición para AWS Cost Explorer Service
- Acciones, recursos y claves de condición para el Centro de optimización de costos de AWS
- Acciones, recursos y claves de condición para el Servicio de verificación de clientes de AWS
- Acciones, recursos y claves de condición para AWS Data Exchange
- Claves de condición, recursos y acciones de Amazon Data Lifecycle Manager
- Acciones, recursos y claves de condición para AWS Data Pipeline
- Acciones, recursos y claves de condición para AWS Database Migration Service
- Claves de condición, recursos y acciones de Database Query Metadata Service

- Acciones, recursos y claves de condición para AWS DataSync
- Acciones, recursos y claves de condición de Amazon DataZone
- Acciones, recursos y claves de condición para AWS Deadline Cloud
- Acciones, recursos y claves de condición para AWS DeepComposer
- Acciones, recursos y claves de condición para AWS DeepRacer
- Acciones, recursos y claves de condición de Amazon Detective
- Acciones, recursos y claves de condición para AWS Device Farm
- Acciones, recursos y claves de condición de Amazon DevOps Guru
- Acciones, recursos y claves de condición de las herramientas AWS Diagnostic
- Acciones, recursos y claves de condición para AWS Direct Connect
- Acciones, recursos y claves de condición para AWS Directory Service
- Acciones, recursos y claves de condición para AWS Directory Service Data
- Acciones, recursos y claves de condición para Amazon DocumentDB Elastic Clusters
- Acciones, recursos y claves de condición para Amazon DynamoDB
- Claves de condición, recursos y acciones para Amazon DynamoDB Accelerator (DAX)
- Claves de condición, recursos y acciones de Amazon EC2 Auto Scaling
- Claves de condición, recursos y acciones de Amazon EC2 Image Builder
- Acciones, recursos y claves de condición de Amazon EC2 Instance Connect
- Acciones, recursos y claves de condición para Amazon EKS Auth
- Acciones, recursos y claves de condición para AWS Elastic Beanstalk
- Acciones, recursos y claves de condición para Amazon Elastic Block Store
- Acciones, recursos y claves de condición para Amazon Elastic Container Registry
- Acciones, recursos y claves de condición de Amazon Elastic Container Registry Public
- Claves de condición, recursos y acciones de Amazon Elastic Container Service
- Acciones, recursos y claves de condición para AWS Elastic Disaster Recovery.
- Claves de condición, recursos y acciones de Amazon Elastic File System
- Acciones, recursos y claves de condición para Amazon Elastic Kubernetes Service
- Acciones, recursos y claves de condición para AWS Elastic Load Balancing
- Acciones, recursos y claves de condición para AWS Elastic Load Balancing V2

- Claves de condición, recursos y acciones de Amazon Elastic MapReduce
- Acciones, recursos y claves de condición de Amazon Elastic Transcoder
- Claves de condición, recursos y acciones de Amazon Elastic VMware Service
- Acciones, recursos y claves de condición de Amazon ElastiCache
- Acciones, recursos y claves de condición para AWS Elemental Appliances and Software
- Acciones, recursos y claves de condición para el servicio de activación de software y dispositivos de AWS Elemental
- Claves de acción, recursos y condiciones de AWS Elemental MediaConnect
- Claves de acción, recursos y condiciones de AWS Elemental MediaConvert
- Claves de acción, recursos y condiciones de AWS Elemental MediaLive
- Claves de acción, recursos y condiciones de AWS Elemental MediaPackage
- Claves de acciones, recursos y condiciones de AWS Elemental MediaPackage V2
- Claves de acciones, recursos y condiciones de AWS Elemental MediaPackage VOD
- Claves de acción, recursos y condiciones de AWS Elemental MediaStore
- Claves de acción, recursos y condiciones de AWS Elemental MediaTailor
- Acciones, recursos y claves de condición para AWS Elemental Support Cases
- Acciones, recursos y claves de condición para AWS Elemental Support Content
- Acciones, recursos y claves de condición para Amazon EMR on EKS (EMR Containers)
- Acciones, recursos y claves de condición para Amazon EMR Serverless
- Claves de acciones, recursos y condiciones para la mensajería de usuario AWS final (SMS y voz) (versión 2)
- Acciones, recursos y claves de condición para Mensajes de redes sociales para usuarios finales de AWS
- Acciones, recursos y claves de condición para AWS Entity Resolution
- Acciones, recursos y claves de condición de Amazon EventBridge
- Acciones, recursos y claves de condición de Amazon EventBridge Pipes
- Claves de condición, recursos y acciones de Amazon EventBridge Scheduler
- Claves de condición, recursos y acciones de Amazon EventBridge Schemas
- Acciones, recursos y claves de condición para el servicio de inserción de errores de AWS

- Acciones, recursos y claves de condición de Amazon FinSpace
- Claves de condición, recursos y acciones de la FinSpace API de Amazon
- Acciones, recursos y claves de condición para AWS Firewall Manager
- Acciones, recursos y claves de condición para Amazon Forecast
- Acciones, recursos y claves de condición para Amazon Fraud Detector
- Acciones, recursos y claves de condición para el nivel gratuito de AWS
- Acciones, recursos y claves de condición para Amazon FreeRTOS
- Acciones, recursos y claves de condición de Amazon FSx
- Claves de condición, recursos y acciones para Amazon GameLift Servers
- Claves de condición, recursos y acciones de Amazon GameLift Streams
- Acciones, recursos y claves de condición para AWS Global Accelerator
- Acciones, recursos y claves de condición para AWS Glue
- Acciones, recursos y claves de condición de AWS Glue DataBrew
- Acciones, recursos y claves de condición para AWS Ground Station
- Acciones, recursos y claves de condición para Amazon GroundTruth Labeling
- Acciones, recursos y claves de condición de Amazon GuardDuty
- Acciones, recursos y claves de estado para AWS Health APIs and Notifications
- Acciones, recursos y claves de condición para AWS HealthImaging
- Acciones, recursos y claves de condición para AWS HealthLake
- Acciones, recursos y claves de condición para AWS HealthOmics
- Acciones, recursos y claves de condición para Amazon Honeycode
- Acciones, recursos y claves de condición para AWS IAM Access Analyzer
- Claves de acciones, recursos y condiciones del AWS IAM Identity Center
- Claves de condición, recursos y acciones para el directorio del Centro de Identidad de AWS IAM
- Acciones, recursos y claves de condición para el servicio OIDC del Centro de Identidad de IAM de AWS
- Acciones, recursos y claves de condición para AWS Identity and Access Management (IAM)
- Acciones, recursos y claves de condición para AWS Identity and Access Management Roles Anywhere

- Acciones, recursos y claves de condición para el almacén de identidades de AWS
- Acciones, recursos y claves de condición para AWS Identity Store Auth
- Acciones, recursos y claves de condición para AWS Identity Synch
- Acciones, recursos y claves de condición para AWS Import Export Disk Service
- Acciones, recursos y claves de condición para Amazon Inspector
- Acciones, recursos y claves de condición para Amazon Inspector2
- Acciones, recursos y claves de condición de Amazon InspectorScan
- Acciones, recursos y claves de condición para Amazon Interactive Video Service
- Acciones, recursos y claves de condición para Amazon Interactive Video Service Chat
- Acciones, recursos y claves de condición para AWS Invoicing Service
- Acciones, recursos y claves de condición para AWS IoT 1-Click
- Acciones, recursos y claves de condición para AWS IoT Analytics
- Acciones, recursos y claves de condición para AWS IoT Core Device Advisor
- Acciones, recursos y claves de condición para AWS IoT Device Tester
- Acciones, recursos y claves de condición para AWS IoT Events
- Acciones, recursos y claves de condición para AWS IoT Fleet Hub para la administración de dispositivos
- Claves de condiciones, recursos y acciones para el AWS IoT FleetWise
- Acciones, recursos y claves de condición para AWS IoT Greengrass
- Acciones, recursos y claves de condición para AWS IoT Greengrass V2
- Acciones, recursos y claves de condición para los trabajos de AWS IoT DataPlane
- Claves de condiciones, recursos y acciones para las integraciones gestionadas de AWS IoT
- Claves de condiciones, recursos y acciones para el AWS IoT SiteWise
- Claves de condiciones, recursos y acciones para el AWS IoT TwinMaker
- Acciones, recursos y claves de condición para AWS IoT Wireless
- Acciones, recursos y claves de condición para AWS IQ
- Acciones, recursos y claves de condición para AWS IQ Permissions
- Acciones, recursos y claves de condición para Amazon Kendra
- Acciones, recursos y claves de condición para Amazon Kendra Intelligent Ranking

- Acciones, recursos y claves de condición de Amazon Keyspaces (for Apache Cassandra)
- Acciones, recursos y claves de condición para Amazon Kinesis Analytics
- Acciones, recursos y claves de condición para Amazon Kinesis Analytics V2
- Acciones, recursos y claves de condición para Amazon Kinesis Data Streams
- Acciones, recursos y claves de condición para Amazon Kinesis Firehose
- Acciones, recursos y claves de condición para Amazon Kinesis Video Streams
- Acciones, recursos y claves de condición para AWS Lake Formation
- Acciones, recursos y claves de condición para AWS Lambda
- Acciones, recursos y claves de condición para AWS Launch Wizard
- Acciones, recursos y claves de condición para Amazon Lex
- Acciones, recursos y claves de condición para Amazon Lex V2
- Acciones, recursos y claves de condición para AWS License Manager
- Acciones, recursos y claves de condición para AWS License Manager Linux Subscriptions Manager
- Acciones, recursos y claves de condición para AWS License Manager User Subscriptions
- Acciones, recursos y claves de condición para Amazon Lightsail
- Acciones, recursos y claves de condición para Amazon Location
- Claves de estado, recursos y acciones de Amazon Location Service Maps
- Acciones, recursos y claves de condición de Amazon Location Service Places
- Claves de estado, recursos y acciones de Amazon Location Service Routes
- Acciones, recursos y claves de condición para Amazon Lookout for Equipment
- Acciones, recursos y claves de condición para Amazon Lookout for Metrics
- Acciones, recursos y claves de condición para Amazon Lookout for Vision
- Acciones, recursos y claves de condición para Amazon Machine Learning
- Acciones, recursos y claves de condición para Amazon Macie
- Acciones, recursos y claves de condición para las Pruebas de aplicaciones de AWS Mainframe Modernization
- Acciones, recursos y claves de condición para AWS Mainframe Modernization Service
- Acciones, recursos y claves de condición para Amazon Managed Blockchain

- Acciones, recursos y claves de condición para Amazon Managed Blockchain Query
- Acciones, recursos y claves de condición para Amazon Managed Grafana
- Acciones, recursos y claves de condición para Amazon Managed Service for Prometheus
- Acciones, recursos y claves de condición para Amazon Managed Streaming for Apache Kafka.
- Acciones, recursos y claves de condición para Amazon Managed Streaming for Kafka Connect
- Acciones, recursos y claves de condición para Amazon Managed Workflows for Apache Airflow
- Acciones, recursos y claves de condición para AWS Marketplace
- Acciones, recursos y claves de condición para AWS Marketplace Catalog
- Acciones, recursos y claves de condición para el servicio de análisis de comercio de AWS Marketplace
- Acciones, recursos y claves de condición para el servicio de implementación de AWS Marketplace
- Acciones, recursos y claves de condición para AWS Marketplace Discovery
- Acciones, recursos y claves de condición para el servicio de concesión de derechos de AWS Marketplace
- Acciones, recursos y claves de condición para el servicio de compilación de imágenes de AWS Marketplace
- Acciones, recursos y claves de condición para AWS Marketplace Management Portal
- Acciones, recursos y claves de condición para el servicio de medición de AWS Marketplace
- Acciones, recursos y claves de condición para AWS Marketplace Private Marketplace
- Acciones, recursos y claves de condición para la integración de sistemas de adquisición de AWS Marketplace
- Acciones, recursos y claves de condición para los Informes de AWS Marketplace
- Claves de condición, recursos y acciones para AWS Marketplace Seller Reporting
- Acciones, recursos y claves de condición para AWS Marketplace Vendor Insights
- Acciones, recursos y claves de condición para Amazon Mechanical Turk
- Acciones, recursos y claves de condición para Amazon MemoryDB
- Acciones, recursos y claves de condición para el Servicio de entrega de mensajes de Amazon
- Acciones, recursos y claves de condición para el Servicio de puerta de enlace de mensajes de Amazon
- Acciones, recursos y claves de condición para AWS Microservice Extractor for .NET

- Acciones, recursos y claves de condición para los Créditos del programa de aceleración de la migración de AWS
- Acciones, recursos y claves de condición para AWS Migration Hub
- Acciones, recursos y claves de condición para AWS Migration Hub Orchestrator
- Acciones, recursos y claves de condición para AWS Migration Hub Refactor Spaces
- Acciones, recursos y claves de condición para AWS Migration Hub Strategy Recommendations
- Acciones, recursos y claves de condición para Amazon Mobile Analytics
- Acciones, recursos y claves de condición para Amazon Monitron
- Acciones, recursos y claves de condición para Amazon MQ
- Claves de condición, recursos y acciones para la aprobación por parte de varias partes
- Acciones, recursos y claves de condición de Amazon Neptune
- Acciones, recursos y claves de condición para Analítica de Amazon Neptune
- Acciones, recursos y claves de condición para AWS Network Firewall
- Claves de acciones, recursos y condición del Monitor de flujo de red
- Acciones, recursos y claves de condición para el Administrador de red de AWS
- Acciones, recursos y claves de condición para el chat del Administrador de red de AWS
- Acciones, recursos y claves de condición para Amazon Nimble Studio
- Acciones, recursos y claves de condición para Amazon One Enterprise
- Acciones, recursos y claves de condición de Amazon OpenSearch
- Claves de condición, recursos y acciones de Amazon OpenSearch Ingestion
- Claves de condición, recursos y acciones de Amazon OpenSearch Serverless
- Acciones, recursos y claves de condición de Amazon OpenSearch Service
- Acciones, recursos y claves de condición para AWS OpsWorks
- Claves de condición, recursos y acciones para la administración AWS OpsWorks de la configuración
- Acciones, recursos y claves de condición para AWS Organizations
- Acciones, recursos y claves de condición para AWS Outposts
- Acciones, recursos y claves de condición para AWS Panorama
- Acciones, recursos y claves de condición para AWS Parallel Computing Service

- Acciones, recursos y claves de condición para la administración de cuenta central de AWS Partner
- Claves de acciones, recursos y condiciones de AWS Partner Central Selling
- Acciones, recursos y claves de condición para Criptografía de pagos de AWS
- Acciones, recursos y claves de condición para AWS Payments
- Acciones, recursos y claves de condición para AWS Performance Insights
- Acciones, recursos y claves de condición para Amazon Personalize
- Acciones, recursos y claves de condición para Amazon Pinpoint
- Acciones, recursos y claves de condición para Amazon Pinpoint Email Service
- Acciones, recursos y claves de condición para Amazon Pinpoint SMS and Voice Service
- Acciones, recursos y claves de condición para Amazon Polly
- Acciones, recursos y claves de condición para AWS Price List
- Acciones, recursos y claves de condición de AWS Private CA Connector for Active Directory
- Acciones, recursos y claves de condición para el Conector de AWS Private CA para SCEP
- Acciones, recursos y claves de condición para AWS Private Certificate Authority
- Acciones, recursos y claves de condición para AWS PrivateLink
- Acciones, recursos y claves de condición para AWS Proton
- Acciones, recursos y claves de condición para AWS Purchase Orders Console
- Acciones, recursos y claves de condición para Amazon Q
- Acciones, recursos y claves de condición para Amazon Q Business
- Acciones, recursos y claves de condición para las aplicaciones de Q de Amazon Q Business
- Acciones, recursos y claves de condición para Amazon Q Developer
- Acciones, recursos y claves de condición para Amazon Q in Connect
- Acciones, recursos y claves de condición para Amazon QLDB
- Acciones, recursos y claves de condición de Amazon QuickSight
- Acciones, recursos y claves de condición de la API de datos de Amazon RDS
- Acciones, recursos y claves de condición para la autenticación IAM de Amazon RDS
- Acciones, recursos y claves de condición para la papelera de reciclaje de AWS
- Acciones, recursos y claves de condición para Amazon Redshift

- Acciones, recursos y claves de condición para la API de datos de Amazon Redshift
- Acciones, recursos y claves de condición para Amazon Redshift sin servidor
- Acciones, recursos y claves de condición de Amazon Rekognition
- Claves de acción, recursos y condición de AWS RePost Private
- Acciones, recursos y claves de condición para AWS Resilience Hub
- Acciones, recursos y claves de condición para Administrador de acceso a recursos de AWS (RAM)
- Acciones, recursos y claves de condición para AWS Resource Explorer
- Claves de condición, recursos y acciones de la API de etiquetado de grupos de recursos de Amazon
- Acciones, recursos y claves de condición para AWS Resource Groups
- Acciones, recursos y claves de condición para Amazon RHEL Knowledgebase Portal
- Acciones, recursos y claves de condición para AWS RoboMaker
- Acciones, recursos y claves de condición para Amazon Route 53
- Acciones, recursos y claves de condición para Amazon Route 53 Domains
- Acciones, recursos y claves de condición para los Perfiles de Amazon Route 53
- Acciones, recursos y claves de condición para Amazon Route 53 Recovery Cluster
- Acciones, recursos y claves de condición para Amazon Route 53 Recovery Controls
- Acciones, recursos y claves de condición para Amazon Route 53 Recovery Readiness
- Acciones, recursos y claves de condición para Amazon Route 53 Resolver
- Acciones, recursos y claves de condición para Amazon S3 Express
- Acciones, recursos y claves de condición para Amazon S3 Glacier
- Claves de condición, acciones y recursos de Amazon S3 Object Lambda
- Acciones, recursos y claves de condición de Amazon S3 en Outposts
- Claves de condición, recursos y acciones para Amazon S3 Tables
- Claves de condiciones, recursos y acciones del asistente de ciencia SageMaker de datos de Amazon
- Claves de condiciones, recursos y acciones para las capacidades SageMaker geoespaciales de Amazon
- Acciones, recursos y claves de condición para Amazon SageMaker con MLflow

- Acciones, recursos y claves de condición para AWS Savings Plans
- Acciones, recursos y claves de condición para AWS Secrets Manager
- Acciones, recursos y claves de condición para AWS Security Hub
- Claves de condiciones, recursos y acciones para la respuesta a incidentes AWS de seguridad
- Acciones, recursos y claves de condición para Amazon Security Lake
- Acciones, recursos y claves de condición para AWS Server Migration Service
- Acciones, recursos y claves de condición para AWS Serverless Application Repository
- Claves de condición, recursos y acciones de AWS Service - Oracle Database@AWS
- Acciones, recursos y claves de condición para AWS Service Catalog
- Acciones, recursos y claves de condición para AWS service providing managed private networks
- Acciones, recursos y claves de condición para Service Quotas
- Claves de condición, recursos y acciones de Amazon SES
- Acciones, recursos y claves de condición para AWS Shield
- Acciones, recursos y claves de condición para AWS Signer
- Acciones, recursos y claves de condición para AWS Signin
- Acciones, recursos y claves de condición para Amazon Simple Email Service - Administrador de correo electrónico
- Acciones, recursos y claves de condición para Amazon Simple Email Service v2
- Acciones, recursos y claves de condición para Amazon Simple Workflow Service
- Acciones, recursos y claves de condición de Amazon SimpleDB
- Claves de condición, recursos y acciones de AWS SimSpace Weaver
- Acciones, recursos y claves de condición para AWS Snow Device Management
- Acciones, recursos y claves de condición para AWS Snowball
- Acciones, recursos y claves de condición para Amazon SNS
- Acciones, recursos y claves de condiciones para SQL Workbench AWS
- Acciones, recursos y claves de condición para Amazon SQS
- Acciones, recursos y claves de condición para AWS Step Functions
- Acciones, recursos y claves de condición para AWS Storage Gateway
- Claves de condición, recursos y acciones para AWS Supply Chain

- Acciones, recursos y claves de condición para AWS Support
- Acciones, recursos y claves de condición para AWS Support App en Slack
- Acciones, recursos y claves de condición para AWS Support Console
- Acciones, recursos y claves de condición para AWS Support Plans
- Acciones, recursos y claves de condición para las Recomendaciones de AWS Support
- Acciones, recursos y claves de condición para AWS Sustainability
- Acciones, recursos y claves de condición para AWS Systems Manager
- Acciones, recursos y claves de condición para AWS Systems Manager para SAP
- Acciones, recursos y claves de condición para AWS Systems Manager GUI Connect
- Acciones, recursos y claves de condición para AWS Systems Manager Incident Manager
- Acciones, recursos y claves de condición para AWS Systems Manager Incident Manager Contacts
- Acciones, recursos y claves de condición para la Configuración Rápida de AWS Systems Manager
- Actions, resources, and condition keys for Tag Editor
- Acciones, recursos y claves de condición para la configuración fiscal de AWS
- Acciones, recursos y claves de condición para AWS Telco Network Builder
- Acciones, recursos y claves de condición para Amazon Textract
- Acciones, recursos y claves de condición para Amazon Timestream
- Acciones, recursos y claves de condición para Amazon Timestream InfluxDB
- Acciones, recursos y claves de condición para AWS Tiros
- Acciones, recursos y claves de condición para Amazon Transcribe
- Claves de condición, acciones y recursos para AWS Transfer Family
- Claves de condición, recursos y acciones de AWS Transform
- Acciones, recursos y claves de condición para Amazon Translate
- Acciones, recursos y claves de condición para AWS Trusted Advisor
- Acciones, recursos y claves de condición para Notificaciones de usuario de AWS
- Acciones, recursos y claves de condición para Contactos de notificaciones de usuario de AWS
- Acciones, recursos y claves de condición para AWS User Subscriptions
- Acciones, recursos y claves de condición para Acceso verificado de AWS
- Acciones, recursos y claves de condición para Amazon Verified Permissions

- Acciones, recursos y claves de condición de Amazon VPC Lattice
- Acciones, recursos y claves de condición para Amazon VPC Lattice Services
- Acciones, recursos y claves de condición para AWS WAF
- Acciones, recursos y claves de condición para AWS WAF Regional
- Acciones, recursos y claves de condición para AWS WAF V2
- Acciones, recursos y claves de condición para AWS Well-Architected Tool
- Acciones, recursos y claves de condición para AWS Wickr
- Acciones, recursos y claves de condición de Amazon WorkDocs
- Acciones, recursos y claves de condición de Amazon WorkLink
- Acciones, recursos y claves de condición de Amazon WorkMail
- Claves de condición, recursos y acciones de Amazon WorkMail Message Flow
- Acciones, recursos y claves de condición de Amazon WorkSpaces
- Acciones, recursos y claves de condición de Amazon WorkSpaces Application Manager
- Claves de condición, recursos y acciones de las instancias AWS WorkSpaces gestionadas
- Claves de condición, recursos y acciones de Amazon WorkSpaces Secure Browser
- Claves de condición, recursos y acciones de Amazon WorkSpaces Thin Client
- Acciones, recursos y claves de condición para AWS X-Ray

Claves de condición, acciones y recursos para AWS Account Management

AWS La administración de cuentas (prefijo de servicio:`account`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Account Management
- Tipos de recursos definidos por AWS Account Management
- Claves de condición para AWS Account Management

Acciones definidas por AWS Account Management

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptPrimaryEmailUpdate	Otorga permiso para aceptar el proceso de actualización de la dirección de correo electrónico principal de una cuenta	Escritura	accountInOrganization		
				account:EmailTargetDomain	
CloseAccount [solo permiso]	Concede permiso para cerrar una cuenta	Escritura	account		
DeleteAlternateContact	Otorga permiso para eliminar los contactos alternativos de una cuenta	Escritura	account		
			accountInOrganization		
				account:AlternateContactTypes	
DisableRegion	Otorga permiso para desactivar una región	Escritura	account		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			accountInOrganization		
				account:TargetRegion	
EnableRegion	Otorga permiso para habilitar una región	Escritura	account		
			accountInOrganization		
				account:TargetRegion	
GetAccountInformation	Concede permiso para recuperar la información de una cuenta	Lectura	account		
			accountInOrganization		
GetAlternateContact	Otorga permiso para recuperar los contactos alternativos de una cuenta	Lectura	account		
			accountInOrganization		
				account:AlternateContactTypes	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetContactInformation	Otorga permiso para recuperar la información de contacto principal para una cuenta	Lectura	account		
			accountInOrganization		
GetPrimaryEmail	Otorga permiso para recuperar la dirección de correo electrónico principal de una cuenta	Lectura	accountInOrganization		
GetRegionOptStatus	Otorga permiso para obtener el estado de participación de una región	Lectura	account		
			accountInOrganization		
				account:TargetRegion	
ListRegions	Otorga permiso para enumerar las regiones disponibles	Enumeración	account		
			accountInOrganization		
PutAccountName	Otorga permiso para actualizar el nombre de una cuenta	Escritura	account		
			accountInOrganization		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutAlternateContact	Otorga permiso para modificar los contactos alternativos de una cuenta	Escritura	account		
			accountInOrganization		
				account:AlternateContactTypes	
PutContactInformation	Otorga permiso para actualizar la información de contacto principal para una cuenta	Escritura	account		
			accountInOrganization		
StartPrimaryEmailUpdate	Otorga permiso para iniciar el proceso de actualización de la dirección de correo electrónico principal de una cuenta	Escritura	accountInOrganization		
				account:EmailTargetDomain	

Tipos de recursos definidos por AWS Account Management

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
account	`arn:${Partition}:account::${Account}:account`	
accountInOrganization	`arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}`	

Claves de condición para AWS Account Management

AWS La administración de cuentas define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
account:AccountResourceOrgPaths	Filtra el acceso por la ruta de recursos de una cuenta en una organización	ArrayOfString
account:AccountResourceOrgTags/${TagKey}	Filtra el acceso por las etiquetas de recursos de una cuenta en una organización	Cadena
account:AlternateContactTypes	Filtra el acceso por los tipos de contacto alternativos	ArrayOfString

Claves de condición	Descripción	Tipo
account:EmailTargetDomain	Filtra el acceso por dominio de correo electrónico de la dirección de correo electrónico de destino	Cadena
account:TargetRegion	Filtra el acceso por una lista de las regiones. Habilita o deshabilita todas las regiones especificadas aquí	Cadena

Acciones, recursos y claves de condición para AWS Activate

AWS Activate (prefijo de servicio:`activate`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Activate
- Tipos de recursos definidos por AWS Activate
- Claves de condición para AWS Activate

Acciones definidas por AWS Activate

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateForm	Otorga permiso para enviar un formulario de solicitud de Activate	Escritura			
GetAccountContact	Otorga permiso para obtener la información de Cuenta de AWS contacto	Lectura			
GetContentInfo	Otorga permiso para obtener publicaciones técnicas de Activate y ofrecer información	Lectura			
GetCosts	Otorga permiso para obtener la información sobre los AWS costos	Lectura			
GetCredits	Otorga permiso para obtener la información AWS crediticia	Lectura			
GetMemberInfo	Otorga permiso para obtener la información del miembro de Activate	Read			
GetProgram	Otorga permiso para obtener un programa de Activate	Read			
PutMemberInfo	Otorga permiso para crear o actualizar la información de miembro de Activate	Write			

Tipos de recursos definidos por AWS Activate

AWS Activate no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Activate, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Activate

Activate no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condiciones, recursos y acciones para Amazon AI Operations

Amazon AI Operations (prefijo de servicio:`aiops`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon AI Operations
- Tipos de recursos definidos por Amazon AI Operations
- Claves de condición de Amazon AI Operations

Acciones definidas por Amazon AI Operations

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInvestigation	Otorga permiso para crear una nueva investigación en el grupo de investigación especificado	Escritura	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
CreateInvestigationEvent	Otorga permiso para crear un nuevo evento de investigación en el grupo de investigación especificado	Escritura	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:Decrypt kms:GenerateDataKey

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					logs:GetQueryResults sts:SetContext

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInvestigationGroup	Otorga permiso para crear un nuevo grupo de investigación	Escritura		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	aiops:TagResource cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInvestigationResource	Otorga permiso para crear un recurso de investigación en el grupo de investigación especificado	Escritura	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:GenerateDataKey logs:GetQueryResults
DeleteInvestigation	Otorga permiso para eliminar una investigación del grupo de investigación especificado	Escritura	investigation-group*		sts:SetContext
DeleteInvestigationGroup	Otorga permiso para eliminar el grupo de investigación especificado	Escritura	investigation-group*		sso:DeleteApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteInvestigationGroupPolicy	Otorga permiso para eliminar la política del grupo de investigación asociada a un grupo de investigación	Escritura	investigation-group*		
GetInvestigation	Otorga permiso para recuperar una investigación del grupo de investigación especificado	Lectura	investigation-group*		
GetInvestigationEvent	Otorga permiso para recuperar un evento de investigación en el grupo de investigación especificado	Lectura	investigation-group*		kms:Decrypt
GetInvestigationGroup	Otorga permiso para recuperar el grupo de investigación especificado	Lectura	investigation-group*		
GetInvestigationGroupPolicy	Otorga permiso para recuperar la política de un grupo de investigación vinculada a un grupo de investigación	Lectura	investigation-group*		
GetInvestigationResource	Otorga permiso para recuperar un recurso de investigación del grupo de investigación especificado	Lectura	investigation-group*		kms:Decrypt

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListInvestigationEvents	Otorga permiso para enumerar todos los eventos de investigación del grupo de investigación especificado	Enumeración	investigation-group*		
ListInvestigationGroups	Otorga permiso para incluir todos los grupos de investigación al Cuenta de AWS presentar la solicitud	Enumeración			
ListInvestigations	Otorga permiso para incluir en una lista todas las investigaciones que se encuentran en el grupo de investigación especificado	Enumeración	investigation-group*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso especificado	Enumeración	investigation-group*		
PutInvestigationGroupPolicy	Otorga permiso a create/update la política de grupo de investigación vinculada a un grupo de investigación	Escritura	investigation-group*		
TagResource	Otorga permiso para agregar o actualizar las etiquetas especificadas para el recurso especificado	Etiquetado	investigation-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para quitar las etiquetas especificadas de los recursos especificados	Etiquetado	investigation-group*		
				aws:TagKeys	
UpdateInvestigation	Otorga permiso para actualizar una investigación en el grupo de investigación especificado	Escritura	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
UpdateInvestigationEvent	Otorga permiso para actualizar un evento de investigación en el grupo de investigación especificado	Escritura	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateInvestigationGroup	Otorga permiso para actualizar el grupo de investigación especificado	Escritura	investigation-group*		cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope sso:PutApplicationAssignmen

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					tConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource
ValidateInvestigationGroup	Otorga permiso para validar el grupo de investigación especificado	Lectura	investigation-group*		

Tipos de recursos definidos por Amazon AI Operations

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
investigation-group	`arn:${Partition}:aiops:${Region}:${Account}:investigation-group/${InvestigationGroupId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon AI Operations

Amazon AI Operations define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Alexa for Business

Alexa for Business (prefijo de servicio: `a4b`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Alexa for Business
- Tipos de recursos definidos por Alexa for Business
- Claves de condición para Alexa for Business

Acciones definidas por Alexa for Business

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApproveSkill	Otorga permiso para asociar una habilidad a la organización bajo la dirección del cliente Cuenta de AWS	Escritura			
AssociateContactWithAddressBook	Concede permiso para asociar un contacto con una libreta de direcciones determinada	Write	addressbook*		
			contact*		
AssociateDeviceWithNetworkProfile	Concede permiso para asociar un dispositivo con el perfil de red especificado	Write	device*		
			networkprofile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateDeviceWithRoom	Concede permiso para asociar un dispositivo con una sala determinada	Write	device* room*		
AssociateSkillGroupWithRoom	Concede permiso para asociar el grupo de habilidades a una habitación determinada	Write	room* skillgroup*		
AssociateSkillWithSkillGroup	Concede permiso para asociar una habilidad a un grupo de habilidades	Write	skillgroup*		
AssociateSkillWithUsers	Concede permiso para poner una habilidad privada a disposición de los usuarios inscritos para que la habiliten en sus dispositivos	Write			
CompleteRegistration [solo permiso]	Concede permiso para completar la operación de registro de un dispositivo Alexa	Write			
CreateAddressBook	Concede permiso para crear una libreta de direcciones con los detalles especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBusinessReportSchedule	Concede permiso para crear una programación recurrente para entregar informes de uso a la ubicación especificada de S3 con un intervalo diario o semanal determinado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConferenceProvider	Otorga permiso para añadir un nuevo proveedor de conferencias bajo el nombre del usuario Cuenta de AWS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContact	Concede permiso para crear un contacto con los detalles especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGatewayGroup	Concede permiso para crear un grupo de gateway con los detalles especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkProfile	Concede permiso para crear un perfil de red con los detalles especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProfile	Concede permiso para crear un nuevo proyecto	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoom	Concede permiso para crear una sala con los detalles especificados	Write	profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSkillGroup	Concede permiso para crear un grupo de habilidades con nombre y descripción dados	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Concede permiso para crear un usuario	Write	user*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAddressBook	Concede permiso para eliminar una libreta de direcciones por el ARN de la libreta de direcciones	Write	addressbook*		
DeleteBusinessReportSchedule	Concede permiso para eliminar la programación recurrente de entrega de informes con el ARN de programación especificado	Write	schedule*		
DeleteConferenceProvider	Concede permiso para eliminar un proveedor de conferencia	Write	conferenceprovider*		
DeleteContact	Concede permiso para eliminar un contacto mediante el ARN de contactos	Write	contact*		
DeleteDevice	Concede permiso para quitar un dispositivo de Alexa For Business	Write	device*		
DeleteDeviceUsageData	Concede permiso para eliminar todo el historial anterior del dispositivo de datos de entrada de voz y datos de respuesta asociados	Write	device*		
DeleteGatewayGroup	Concede permiso para eliminar un grupo de gateway	Write	gatewaygroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteNetworkProfile	Concede permiso para eliminar un perfil de red mediante el ARN del perfil de red	Write	networkprofile*		
DeleteProfile	Concede permiso para eliminar perfil mediante el ARN de perfil	Write	profile*		
DeleteRoom	Concede permiso para eliminar una sala	Write	room*		
DeleteRoomSkillParameter	Concede permiso para eliminar un parámetro de una habilidad y una sala	Write	room*		
DeleteSkillAuthorization	Concede permiso para desvincular una cuenta de terceros de una habilidad	Write	room*		
DeleteSkillGroup	Concede permiso para eliminar un grupo de habilidades con ARN del grupo de habilidades	Write	skillgroup*		
DeleteUser	Concede permiso para eliminar un usuario	Write	user*		
DisassociateContactFromAddressBook	Concede permiso para desasociar a un contacto de una libreta de direcciones determinada	Write	addressbook* contact*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateDeviceFromRoom	Concede permiso para desasociar el dispositivo de su sala actual	Write	device*		
DisassociateSkillFromSkillGroup	Concede permiso para desasociar una habilidad de un grupo de habilidades	Write	skillgroup*		
DisassociateSkillFromUsers	Concede permiso para hacer que una habilidad privada deje de estar disponible para los usuarios inscritos y les impide que la habiliten en sus dispositivos	Write	user*		
DisassociateSkillGroupFromRoom	Concede permiso para desasociar al grupo de habilidades de una sala determinada	Write	room* skillgroup*		
ForgetSmartHomeAppliances	Concede permiso para olvidar electrodomésticos inteligentes asociados a una sala	Write	room*		
GetAddressBook	Concede permiso para obtener los detalles de la libreta de direcciones por el ARN de la libreta de direcciones	Read	addressbook*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConferencePreference	Concede permiso para recuperar las preferencias de las conferencia existentes	Read			
GetConferenceProvider	Concede permiso para obtener detalles sobre un proveedor de conferencias específico	Read	conferenceprovider*		
GetContact	Concede permiso para obtener los datos de contacto por el ARN de contacto	Read	contact*		
GetDevice	Concede permiso para obtener detalles del dispositivo	Read	device*		
GetGateway	Concede permiso para recuperar los detalles de una gateway	Read	gateway*		
GetGatewayGroup	Concede permiso para recuperar los detalles de un grupo de gateway	Read	gatewaygroup*		
GetInvitationConfiguration	Concede permiso para recuperar los valores configurados para la plantilla de correo electrónico de invitación de inscripción de usuario	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetNetworkProfile	Concede permiso para obtener los detalles del perfil de red por el ARN del perfil de red	Read	networkprofile*		
GetProfile	Concede permiso para obtener el perfil cuando se proporciona con ARN de perfil	Read	profile*		
GetRoom	Concede permiso para obtener detalles de la sala	Read	room*		
GetRoomSkillParameter	Concede permiso para obtener un parámetro existente que se ha establecido para una habilidad y una sala	Read	room*		
GetSkillGroup	Concede permiso para obtener detalles del grupo de habilidades con ARN del grupo de habilidades	Read	skillgroup*		
ListBusinessReportSchedules	Concede permiso para enumerar los detalles de las programaciones configuradas por un usuario	Enumeración			
ListConferenceProviders	Otorga permiso para incluir a los proveedores de conferencias en una lista específica Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeviceEvents	Concede permiso para enumerar el historial de eventos del dispositivo, incluido el estado de conexión de dispositivo, durante un máximo de 30 días	List	device*		
ListGatewayGroups	Concede permiso para mostrar resúmenes de grupos de gateway	List			
ListGateways	Concede permiso para enumerar resúmenes de gateway	List	gatewaygroup*		
ListSkills	Concede permiso para enumerar habilidades	List			
ListSkillsStoreCategories	Concede permiso para enumerar todas las categorías en la tienda de habilidades Alexa	List			
ListSkillsStoreSkillsByCategory	Concede permiso para enumerar todas las habilidades de la tienda de habilidades de Alexa por categoría	List			
ListSmartHomeAppliances	Concede permiso para enumerar todos los electrodomésticos inteligentes asociados a una sala	List	room*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTags	Concede permiso para enumerar todas las etiquetas para un recurso	Read	device		
			room		
			user		
PutConferencePreference	Concede permiso para establecer las preferencias de conferencia de un proveedor de servicios de conferencias en el nivel de cuenta	Write			
PutDeviceSetupEvents [solo permiso]	Concede permiso para publicar eventos de configuración de dispositivos Alexa	Write			
PutInvitationConfiguration	Concede permiso para configurar la plantilla de correo electrónico para la invitación de inscripción de usuario con los atributos especificados	Write			
PutRoomSkillParameter	Concede permiso para poner un parámetro específico de sala para una habilidad	Write	room*		
PutSkillAuthorization	Concede permiso para vincular la cuenta de un usuario a un proveedor de habilidades de terceros	Write	room*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterAVSDevice	Concede permiso para registrar un dispositivo con tecnología Alexa desarrollado por un fabricante de equipos originales (Original Equipment Manufacturer, OEM) mediante el servicio de voz de Alexa (Alexa Voice Service, AVS).	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDevice [solo permiso]	Concede permiso para registrar un dispositivo Alexa	Escritura			
RejectSkill	Otorga permiso para desvincular una habilidad de la organización bajo la de un usuario Cuenta de AWS	Escritura			
ResolveRoom	Concede permiso para resolver la información de la sala	Read			
RevokeInvitation	Concede permiso para revocar una invitación	Write	user*		
SearchAddressBooks	Concede permiso para buscar en las libretas de direcciones y enumerar las que cumplen un conjunto de criterios de filtrado y ordenación	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchContacts	Concede permiso para buscar contactos y enumerar los que cumplen un conjunto de criterios de filtrado y ordenación	List			
SearchDevices	Concede permiso para buscar dispositivos	List			
SearchNetworkProfiles	Concede permiso para buscar perfiles de red y enumerar los que cumplen un conjunto de criterios de filtrado y ordenación	List			
SearchProfiles	Concede permiso para buscar perfiles	List			
SearchRooms	Concede permiso para buscar salas	List			
SearchSkillGroups	Concede permiso para buscar grupos de habilidades	List			
SearchUsers	Concede permiso para buscar usuarios	List			
SendAnnouncement	Concede permiso para activar un flujo asincrónico para enviar mensajes de texto, SSML o anuncios de audio a salas identificadas por una búsqueda o filtro	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendInvitation	Concede permiso para enviar una invitación a un usuario	Write	user*		
StartDeviceSync	Concede permiso para restaurar el dispositivo y su cuenta a su configuración predeterminada conocida borrando toda la información y los ajustes establecidos por los usuarios anteriores	Write			
StartSmartHomeApplianceDiscovery	Concede permiso para iniciar la detección de los dispositivos de hogar inteligente asociados a la sala	Read	room*		
TagResource	Concede permiso para agregar etiquetas de metadatos a un recurso	Etiquetado	device		
			room		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de metadatos de un recurso	Etiquetado	device		
			room		
			user		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAddressBook	Concede permiso para actualizar los detalles de la libreta de direcciones por el ARN de la libreta	Write	addressbook*		
UpdateBusinessReportSchedule	Concede permiso para actualizar la configuración de la programación de entrega de informes con el ARN de programación especificado	Write	schedule*		
UpdateConferenceProvider	Concede permiso para actualizar la configuración de un proveedor de conferencia existente	Write	conferenceprovider*		
UpdateContact	Concede permiso para actualizar los datos de contacto por el ARN de contacto	Write	contact*		
UpdateDevice	Concede permiso para actualizar el nombre del dispositivo	Write	device*		
UpdateGateway	Concede permiso para actualizar los detalles de una gateway	Write	gateway*		
UpdateGatewayGroup	Concede permiso para actualizar los detalles de un grupo de gateway	Write	gatewaygroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateNetworkProfile	Concede permiso para actualizar un perfil de red mediante el ARN del perfil de red	Write	networkprofile*		
UpdateProfile	Concede permiso para actualizar un perfil existente	Write	profile*		
UpdateRoom	Concede permiso para actualizar detalles de la habitación	Write	room*		
UpdateSkillGroup	Concede permiso para actualizar los detalles del grupo de habilidades con ARN del grupo de habilidades	Write	skillgroup*		

Tipos de recursos definidos por Alexa for Business

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
profile	`arn:${Partition}:a4b:${Region}:${Account}:profile/${ResourceId}`	

Tipos de recurso	ARN	Claves de condición
room	arn:${Partition}:a4b:${Region}:${Account}:room/${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:a4b:${Region}:${Account}:device/${ResourceId}	aws:ResourceTag/${TagKey}
skillgroup	arn:${Partition}:a4b:${Region}:${Account}:skill-group/${ResourceId}	
user	arn:${Partition}:a4b:${Region}:${Account}:user/${ResourceId}	aws:ResourceTag/${TagKey}
addressbook	arn:${Partition}:a4b:${Region}:${Account}:address-book/${ResourceId}	
conferenceprovider	arn:${Partition}:a4b:${Region}:${Account}:conference-provider/${ResourceId}	
contact	arn:${Partition}:a4b:${Region}:${Account}:contact/${ResourceId}	
schedule	arn:${Partition}:a4b:${Region}:${Account}:schedule/${ResourceId}	
networkprofile	arn:${Partition}:a4b:${Region}:${Account}:network-profile/${ResourceId}	
gateway	arn:${Partition}:a4b:${Region}:${Account}:gateway/${ResourceId}	
gatewaygroup	arn:${Partition}:a4b:${Region}:${Account}:gateway-group/${ResourceId}	

Claves de condición para Alexa for Business

Alexa for Business define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
a4b:amazonId	Filtra acciones en función del ID de Amazon en la solicitud.	Cadena
a4b:filters_deviceType	Filtra acciones en función del tipo de dispositivo en la solicitud.	ArrayOfString
aws:RequestTag/${TagKey}	Filtra acciones en función del conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado con el recurso.	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de etiquetas obligatorias en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AmazonMediaImport

AmazonMediaImport (prefijo de servicio:`mediaimport`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AmazonMediaImport
- Tipos de recursos definidos por AmazonMediaImport
- Claves de condición de AmazonMediaImport

Acciones definidas por AmazonMediaImport

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDatabaseBinarySnapshot [solo permiso]	Concede permiso para crear una instantánea binaria de base de datos en la cuenta de AWS del cliente	Escritura			

Tipos de recursos definidos por AmazonMediaImport

AmazonMediaImport no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AmazonMediaImport, especifique `"Resource": "*"` en su política.

Claves de condición de AmazonMediaImport

mediaimport no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Amplify

AWS Amplify (prefijo de servicio:`amplify`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Amplify
- Tipos de recursos definidos por AWS Amplify
- Claves de condición para AWS Amplify

Acciones definidas por AWS Amplify

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*).

Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate WebACL	Otorga permiso para asociar una WebACL a un recurso	Escritura	apps*		
CreateApp	Concede permiso para crear una nueva aplicación de Amplify	Escritura	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBackendEnvironment	Concede permiso para crear un nuevo entorno de backend para una aplicación de Amplify	Escritura	apps*		
CreateBranch	Concede permiso para crear una nueva ramificación para una aplicación de Amplify	Escritura	branches*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeployment	Concede permiso para crear una implementación para aplicaciones de implementación manual. (Las aplicaciones no están conectadas al repositorio)	Escritura	branches*		
CreateDomainAssociation	Otorga permiso para crear una nueva DomainAssociation en una aplicación	Escritura	domains*		
CreateWebHook	Concede permiso para crear un nuevo webhook en una aplicación	Escritura	branches*		
DeleteApp	Concede permiso para eliminar una aplicación de Amplify existente por appId	Escritura	apps*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBackendEnvironment	Concede permiso para eliminar una ramificación de una aplicación de Amplify	Escritura	apps*		
DeleteBranch	Concede permiso para eliminar una ramificación de una aplicación de Amplify	Escritura	branches*		
DeleteDomainAssociation	Otorga permiso para eliminar un DomainAssociation	Escritura	domains*		
DeleteJob	Concede permiso para eliminar un trabajo de una ramificación de Amplify parte de una aplicación de Amplify	Escritura	jobs*		
DeleteWebHook	Concede permiso para eliminar un webhook por ID	Escritura	webhooks*		
DisassociateWebACL	Otorga permiso para desasociar una WebACL de un recurso	Escritura	apps*		
GenerateAccessLogs	Concede permiso para generar registros de acceso al sitio web para un intervalo de tiempo específico a través de una URL prefirmada	Escritura	apps*		
GetApp	Concede permiso para recuperar una aplicación de Amplify existente por appId	Lectura	apps*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetArtifactUrl	Concede permiso para recuperar información del artefacto que corresponda a un artifactId	Lectura	apps*		
GetBackendEnvironment	Concede permiso para recuperar un entorno de backend para una aplicación de Amplify	Lectura	apps*		
GetBranch	Concede permiso para recuperar una ramificación de una aplicación de Amplify	Lectura	branches*		
GetDomainAssociation	Concede permiso para recuperar información del dominio que corresponda a un appId y domainName	Lectura	domains*		
GetJob	Concede permiso para obtener un trabajo para una ramificación parte de una aplicación de Amplify	Lectura	jobs*		
GetWebACLForResource	Otorga permiso para recuperar la WebACL asociada a un recurso	Lectura	apps*		
GetWebHook	Concede permiso para recuperar información del webhook que corresponda a un webhookId	Lectura	webhooks*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApps	Concede permiso para enumerar las aplicaciones de Amplify existentes	Enumeración			
ListArtifacts	Concede permiso para enumerar los artefactos con una aplicación, una ramificación, un trabajo y un tipo de artefacto	Enumeración	apps*		
ListBackendEnvironments	Concede permiso para enumerar entornos de backend para una aplicación de Amplify	Enumeración	apps*		
ListBranches	Concede permiso para enumerar las ramificaciones de una aplicación de Amplify	Enumeración	apps*		
ListDomainAssociations	Concede permiso para enumerar los dominios con una aplicación	Enumeración	apps*		
ListJobs	Concede permiso para enumerar los trabajos de una ramificación parte de una aplicación de Amplify	Enumeración	branches*		
ListResourcesForWebACL	Otorga permiso para enumerar los recursos asociados a una WebACL	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para enumerar etiquetas para un recurso de AWS Amplify Console	Lectura	apps		
			branches		
			domains		
			webhooks		
ListWebHooks	Concede permiso para enumerar los webhooks de una aplicación	Enumeración	apps*		
StartDeployment	Concede permiso para iniciar una implementación para aplicaciones de implementación manual. (Las aplicaciones no están conectadas al repositorio)	Escritura	branches*		
StartJob	Concede permiso para iniciar un nuevo trabajo para una ramificación parte de una aplicación de Amplify	Escritura	jobs*		
StopJob	Concede permiso para detener un trabajo que está en curso en una ramificación de Amplify parte de una aplicación de Amplify	Escritura	jobs*		
TagResource	Otorga permiso para etiquetar un recurso de AWS Amplify Console	Etiquetado	apps		
			branches		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			domains		
			webhooks		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso de AWS Amplify Console	Etiquetado	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys	
UpdateApp	Concede permiso para actualizar una aplicación de Amplify existente	Escritura	apps*		
UpdateBranch	Concede permiso para actualizar una ramificación de una aplicación de Amplify	Escritura	branches*		
UpdateDomainAssociation	Otorga permiso para actualizar una DomainAssociation aplicación	Escritura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateWebHook	Concede permiso para actualizar un webhook	Escritura	webhooks*		

Tipos de recursos definidos por AWS Amplify

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

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

Claves de condición para AWS Amplify

AWS Amplify define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por la clave de una etiqueta asociada al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Amplify Admin

AWS Amplify Admin (prefijo de servicio:`amplifybackend`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Amplify Admin

- Tipos de recursos definidos por AWS Amplify Admin
- Claves de condición para AWS Amplify Admin

Acciones definidas por AWS Amplify Admin

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CloneBackend	Otorga permiso para clonar un entorno de backend de Amplify Admin existente en un nuevo entorno backend de Amplify Admin	Write	backend*		
CreateBackend	Otorga permiso para crear un nuevo entorno backend de Amplify Admin por el Amplify appId	Escritura	created-backend*		
CreateBackendAPI	Otorga permiso para crear una API para un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	api*		
			backend*		
			environment*		
CreateBackendAuth	Otorga permiso para crear un recurso de autenticación para un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	auth*		
			backend*		
			environment*		
CreateBackendConfig	Otorga permiso para crear una nueva configuración de	Escritura	config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	backend de Amplify Admin por el Amplify appId				
CreateBackendStorage	Otorga permiso para crear un recurso de almacenamiento backend	Escritura	backend*		
			environment*		
			storage*		
CreateToken	Otorga permiso para crear un token de desafío de Amplify Admin por el appId	Escritura	backend*		
			token*		
DeleteBackend	Otorga permiso para eliminar un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	backend*		
			environment*		
DeleteBackendAPI	Otorga permiso para eliminar una API de un entorno de backend de Amplify Admin existente mediante el uso de AppID y backendEnvironmentName	Escritura	api*		
			backend*		
			environment*		
DeleteBackendAuth	Otorga permiso para eliminar un recurso de autenticación de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	auth*		
			backend*		
			environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBackendStorage	Otorga permiso para eliminar un recurso de almacenamiento backend	Escritura	backend*		
			environment*		
			storage*		
DeleteToken	Otorga permiso para eliminar un token de desafío de Amplify Admin por el appId	Escritura	backend*		
			token*		
GenerateBackendAPIModels	Otorga permiso para generar modelos para una API de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	api*		
			backend*		
			environment*		
GetBackend	Otorga permiso para recuperar un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Lectura	backend*		
			environment*		
GetBackendAPI	Otorga permiso para recuperar una API de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Lectura	api*		
			backend*		
			environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBackendAPIModels	Otorga permiso para recuperar modelos para una API de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Lectura	api*		
			backend*		
			environment*		
GetBackendAuth	Otorga permiso para recuperar un recurso de autenticación de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Lectura	auth*		
			backend*		
			environment*		
GetBackendJob	Otorga permiso para recuperar un trabajo de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Lectura	backend*		
			job*		
GetBackendStorage	Otorga permiso para recuperar un recurso de almacenamiento backend existente	Lectura	backend*		
			environment*		
GetToken	Otorga permiso para recuperar un token de desafío de Amplify Admin por el appId	Lectura	backend*		
			token*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportBackendAuth	Otorga permiso para importar un recurso de autenticación existente de un entorno de backend de Amplify Admin mediante AppID y backendEnvironmentName	Escritura	auth*		
			backend*		
			environment*		
ImportBackendStorage	Otorga permiso para importar un recurso de almacenamiento backend existente	Escritura	backend*		
			environment*		
			storage*		
ListBackendJobs	Otorga permiso para recuperar las tareas de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Enumeración	backend*		
			job*		
ListS3Buckets	Otorga permiso para recuperar buckets de s3	Enumeración			s3:ListAllMyBuckets
RemoveAllBackends	Otorga permiso para eliminar todos los entornos backend de Amplify Admin existentes por el appId	Write	backend*		
			environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveBackendConfig	Otorga permiso para eliminar una configuración de backend de Amplify Admin por el Amplify appId	Escritura	config*		
UpdateBackendAPI	Otorga permiso para actualizar una API de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	api*		
			backend*		
			environment*		
UpdateBackendAuth	Otorga permiso para actualizar un recurso de autenticación de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	auth*		
			backend*		
			environment*		
UpdateBackendConfig	Otorga permiso para actualizar una configuración de backend de Amplify Admin por el Amplify appId	Escritura	config*		
UpdateBackendJob	Otorga permiso para actualizar un trabajo de un entorno de backend de Amplify Admin existente mediante AppID y backendEnvironmentName	Escritura	backend*		
			job*		
UpdateBackendStorage	Otorga permiso para actualizar recurso de almacenamiento backend	Escritura	backend*		
			environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			storage*		

Tipos de recursos definidos por AWS Amplify Admin

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
created-backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/*`	
backend	`arn:${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/*`	

Tipos de recurso	ARN	Claves de condición
job	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/job/*`	
config	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/config/*`	
token	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/challenge/*`	
storage	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/storage/*`	

Claves de condición para AWS Amplify Admin

Amplify Admin no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Amplify UI Builder

AWS Amplify UI Builder (prefijo de servicio:`amplifyuibuilder`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Amplify UI Builder
- Tipos de recursos definidos por AWS Amplify UI Builder
- Claves de condición para AWS Amplify UI Builder

Acciones definidas por AWS Amplify UI Builder

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateComponent	Otorga permiso para crear un componente.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetComponent amplifyuibuilder:TagResource
CreateForm	Otorga permiso para crear un formulario	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetForm

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
CreateTheme	Concede permiso para crear un tema.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource
DeleteComponent	Concede el permiso para eliminar un componente.	Escritura	Component Resource*		amplify:GetApp amplifyuibuilder:UntagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteForm	Otorga permiso para eliminar un formulario	Escritura	FormResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
DeleteTheme	Concede permiso para eliminar un tema	Escritura	ThemeResource*		amplify:GetApp amplifyuibuilder:UntagResource
ExchangeCodeForToken	Otorga permiso para intercambiar un código por un token.	Escritura			
ExportComponents	Otorga permiso para exportar componentes.	Lectura			
ExportForms	Otorga permiso para exportar formularios	Lectura			
ExportThemes	Otorga permiso para exportar temas	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCodegenJob	Otorga permiso para obtener un trabajo de generación de código existente	Lectura	CodegenJobResource*		amplify:GetApp
GetComponent	Otorga permiso para obtener un componente existente.	Lectura	ComponentResource*		amplify:GetApp
GetForm	Otorga permiso para obtener un formulario existente	Lectura	FormResource*		amplify:GetApp
GetMetadata	Otorga permiso para obtener metadatos existentes	Lectura			
GetTheme	Otorga permiso para obtener un tema existente.	Lectura	ThemeResource*		amplify:GetApp
ListCodegenJobs	Otorga permiso para enumerar trabajos de generación de código	Enumeración			amplify:GetApp
ListComponents	Otorga permiso para enumerar componentes.	Enumeración			amplify:GetApp
ListForms	Otorga permiso para enumerar formularios	Enumeración			amplify:GetApp
ListTagsForResource	Otorga permiso para enumerar etiquetas para un nombre de recurso de Amazon (ARN) específico	Enumeración	CodegenJobResource		
			ComponentResource		
			FormResource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ThemeResource		
ListThemes	Otorga permiso para enumerar temas	Enumeración			amplify:GetApp
PutMetadataFlag	Otorga permiso para poner metadatos existentes	Escritura			
RefreshToken	Otorga permiso para actualizar un token de acceso.	Escritura			
ResetMetadataFlag	Otorga permiso para restablecer metadatos existentes	Escritura			
StartCodegenJob	Otorga permiso para comenzar un trabajo de generación de código	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp
TagResource	Otorga permiso para etiquetar el recurso con una clave y un valor de etiqueta	Etiquetado	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para quitar la etiqueta de un recurso con un nombre de recurso de Amazon (ARN) especificado	Etiquetado	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys	
UpdateComponent	Concede el permiso para actualizar una componente.	Escritura	ComponentResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateForm	Otorga permiso para actualizar un formulario	Escritura	FormResource*		amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
UpdateTheme	Concede permiso para actualizar un tema	Escritura	ThemeResource*		amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Tipos de recursos definidos por AWS Amplify UI Builder

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
CodegenJobResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/codegen-jobs/${Id}`	amplifyuibuilder:CodegenJobResourceAppId amplifyuibuilder:CodegenJobResourceEnvironmentName amplifyuibuilder:CodegenJobResourceId aws:ResourceTag/${TagKey}
ComponentResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/components/${Id}`	amplifyuibuilder:ComponentResourceAppId amplifyuibuilder:ComponentResourceEnvironmentName amplifyuibuilder:ComponentResourceId

Tipos de recurso	ARN	Claves de condición
		aws:ResourceTag/${TagKey}
FormResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/forms/${Id}	amplifyuibuilder:FormResourceAppId amplifyuibuilder:FormResourceEnvironmentName amplifyuibuilder:FormResourceId aws:ResourceTag/${TagKey}
ThemeResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/themes/${Id}	amplifyuibuilder:ThemeResourceAppId amplifyuibuilder:ThemeResourceEnvironmentName amplifyuibuilder:ThemeResourceId aws:ResourceTag/${TagKey}

Claves de condición para AWS Amplify UI Builder

AWS Amplify UI Builder define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
amplifyuibuilder:CodegenJobResourceAppId	Filtra el acceso según el ID de la aplicación.	Cadena
amplifyuibuilder:CodegenJobResourceEnvironmentName	Filtra el acceso según el nombre del entorno de backend.	Cadena
amplifyuibuilder:CodegenJobResourceId	Filtra el acceso por el ID de trabajo de generación de código	Cadena
amplifyuibuilder:ComponentResourceAppId	Filtra el acceso según el ID de la aplicación.	Cadena
amplifyuibuilder:ComponentResourceEnvironmentName	Filtra el acceso según el nombre del entorno de backend.	Cadena
amplifyuibuilder:ComponentResourceId	Filtra el acceso según el ID del componente.	Cadena

Claves de condición	Descripción	Tipo
amplifyuibuilder:FormResourceAppId	Filtra el acceso según el ID de la aplicación.	Cadena
amplifyuibuilder:FormResourceEnvironmentName	Filtra el acceso según el nombre del entorno de backend.	Cadena
amplifyuibuilder:FormResourceId	Filtra el acceso por el ID del formulario	Cadena
amplifyuibuilder:ThemeResourceAppId	Filtra el acceso según el ID de la aplicación.	Cadena
amplifyuibuilder:ThemeResourceEnvironmentName	Filtra el acceso según el nombre del entorno de backend.	Cadena
amplifyuibuilder:ThemeResourceId	Filtra el acceso según el ID del tema.	Cadena
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones para clústeres de Apache Kafka APIs para Amazon MSK

Los clústeres de Apache Kafka APIs para Amazon MSK (prefijo de servicio:`kafka-cluster`) proporcionan los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Apache Kafka APIs para los clústeres de Amazon MSK
- Tipos de recursos definidos por Apache Kafka APIs para los clústeres de Amazon MSK
- Claves de condición de los clústeres de Apache Kafka APIs para Amazon MSK

Acciones definidas por Apache Kafka APIs para los clústeres de Amazon MSK

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AlterCluster	Otorga permiso para alterar varios aspectos del clúster, equivalente a la ACL ALTER CLUSTER de Apache Kafka	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster
AlterClusterDynamicConfiguration	Otorga permiso para modificar la configuración dinámica de un clúster, equivalente a la ACL de CLÚSTER ALTER_CONFIGS de Apache Kafka	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	Otorga permiso para unirse a grupos en un clúster, equivalente a la ACL READ GROUP de Apache Kafka	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	Otorga permiso para modificar temas en un clúster, equivalente a la ACL ALTER TOPIC de Apache Kafka	Write	topic*		kafka-cluster:Connect

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					kafka-cluster:DescribeTopic
AlterTopicDynamicConfiguration	Otorga permiso para modificar la configuración dinámica de temas en un clúster, equivalente a la ACL de TEMA ALTER_CONFIGS de Apache Kafka	Escritura	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration
AlterTransactionalId	Otorga permiso para modificar las transacciones IDs en un clúster, lo que equivale a la ACL WRITE TRANSACTIONAL_ID de Apache Kafka	Escritura	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	Otorga permiso para conectarse y autenticarse en el clúster	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTopic	Otorga permiso para crear temas en un clúster, lo que equivale a la ACL CREATE de Apache Kafka CLUSTER/TOPIC	Escritura	topic*		kafka-cluster:Connect
DeleteGroup	Otorga permiso para eliminar grupos de un clúster, equivalente a la ACL DELETE GROUP de Apache Kafka	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
DeleteTopic	Otorga permiso para eliminar temas de un clúster, equivalente a la ACL DELETE TOPIC de Apache Kafka	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	Otorga permiso para describir varios aspectos del clúster, equivalente a la ACL DESCRIBE CLUSTER de Apache Kafka	List	cluster*		kafka-cluster:Connect

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeClusterDynamicConfiguration	Otorga permiso para describir la configuración dinámica de un clúster, equivalente a la ACL de CLÚSTER DESCRIBE_CONFIGS de Apache Kafka	List	cluster*		kafka-cluster:Connect
DescribeGroup	Otorga permiso para describir grupos en un clúster, equivalente a la ACL DESCRIBE GROUP de Apache Kafka	List	group*		kafka-cluster:Connect
DescribeTopic	Otorga permiso para describir temas en un clúster, equivalente a la ACL DESCRIBE TOPIC de Apache Kafka	List	topic*		kafka-cluster:Connect
DescribeTopicDynamicConfiguration	Otorga permiso para describir la configuración dinámica de temas en un clúster, equivalente a la ACL DESCRIBE_CONFIGS TOPIC de Apache Kafka	Enumeración	topic*		kafka-cluster:Connect
DescribeTransactionalId	Otorga permiso para describir las transacciones IDs en un clúster, lo que equivale a la ACL DESCRIBE TRANSACTIONAL_ID de Apache Kafka	Enumeración	transactional-id*		kafka-cluster:Connect

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ReadData	Otorga permiso para leer datos de temas de un clúster, equivalente a la ACL READ TOPIC de Apache Kafka	Read	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	Otorga permiso para escribir datos en temas de un clúster, equivalente a la ACL WRITE TOPIC de Apache Kafka	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteDataIdempotently	Otorga permiso para escribir datos idempotentemente en un clúster, equivalente a la ACL de CLÚSTER IDEMPOTENT_WRITE de Apache Kafka	Escritura	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Tipos de recursos definidos por Apache Kafka APIs para los clústeres de Amazon MSK

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${ClusterUuid}`	aws:ResourceTag/${TagKey}
topic	`arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}`	
group	`arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}`	
transactional-id	`arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}`	

Claves de condición de los clústeres de Apache Kafka APIs para Amazon MSK

Apache Kafka APIs para los clústeres de Amazon MSK define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta asociados al recurso. La clave de contexto de la etiqueta de recurso solo se aplicará al recurso del clúster, no a los temas, los grupos ni a las transacciones IDs	Cadena

Acciones, recursos y claves de condición de Amazon API Gateway

Amazon API Gateway (prefijo de servicio: `execute-api`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon API Gateway
- Tipos de recurso definidos por Amazon API Gateway
- Claves de condición para Amazon API Gateway

Acciones definidas por Amazon API Gateway

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InvalidateCache	Se utiliza para invalidar la caché de API previa solicitud del cliente	Write	execute-api-general*		
Invoke	Se utiliza para invocar una API previa solicitud del cliente	Escritura	execute-api-domain		
			execute-api-general		
ManageConnections	ManageConnections controla el acceso a la API @connections	Escritura	execute-api-general*		

Tipos de recurso definidos por Amazon API Gateway

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
execute-api-general	`arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}`	execute-api:viaDomainArn

Tipos de recurso	ARN	Claves de condición
execute-api-domain	`arn:${Partition}:execute-api:${Region}:${Account}:/domainnames/${DomainName}+${DomainIdentifier}`	

Claves de condición para Amazon API Gateway

Amazon API Gateway define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
execute-api:viaDomainArn	Filtra el acceso por el nombre de dominio ARN desde el que se llama a la API	Cadena

Acciones, recursos y claves de condición para AWS App Mesh

AWS App Mesh (prefijo de servicio:`appmesh`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS App Mesh
- Tipos de recursos definidos por AWS App Mesh
- Claves de condición para AWS App Mesh

Acciones definidas por AWS App Mesh

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGatewayRoute	Otorga permiso para crear una ruta de gateway asociada a una gateway virtual	Write	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	Otorga permiso para crear una malla de servicios	Write	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoute	Otorga permiso para crear una ruta asociada a un enrutador virtual	Write	route*	aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			virtualNode		
CreateVirtualGateway	Otorga permiso para crear una gateway virtual dentro de una malla de servicio	Write	virtualGateway*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualNode	Otorga permiso para crear un nodo virtual dentro de una malla de servicio	Write	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	Otorga permiso para crear un enrutador virtual dentro de una malla de servicio	Write	virtualRouter*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVirtualService	Otorga permiso para crear un servicio virtual dentro de una malla de servicio	Write	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
			virtualRouter		
DeleteGatewayRoute	Otorga permiso para eliminar una ruta de gateway existente	Write	gatewayRoute*		
DeleteMesh	Otorga permiso para eliminar una instantánea existente	Escritura	mesh*		
DeleteMeshPolicy [solo permiso]	Concede permiso para eliminar la política de una malla de control de acceso a la RAM	Escritura	mesh*		
DeleteRoute	Concede el permiso para eliminar una ruta existente	Write	route*		
DeleteVirtualGateway	Otorga permiso para eliminar una gateway virtual existente	Write	virtualGateway*		
DeleteVirtualNode	Otorga permiso para eliminar un nodo virtual existente	Write	virtualNode*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteVirtualRouter	Otorga permiso para eliminar un enrutador virtual existente	Write	virtualRouter*		
DeleteVirtualService	Otorga permiso para eliminar un servicio virtual existente	Write	virtualService*		
DescribeGatewayRoute	Otorga permiso para describir una ruta de gateway existente	Read	gatewayRoute*		
DescribeMesh	Otorga permiso para describir una malla de servicios existente	Read	mesh*		
DescribeRoute	Otorga permiso para describir una ruta existente	Read	route*		
DescribeVirtualGateway	Otorga permiso para describir una gateway virtual existente	Read	virtualGateway*		
DescribeVirtualNode	Otorga permiso para describir un noto virtual existente	Read	virtualNode*		
DescribeVirtualRouter	Otorga permiso para describir un enrutador virtual existente	Read	virtualRouter*		
DescribeVirtualService	Otorga permiso para describir un servicio virtual existente	Lectura	virtualService*		
GetMeshPolicy [solo permiso]	Concede permiso para leer la política de una malla de control de acceso a la RAM	Lectura	mesh*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGatewayRoutes	Otorga permiso para enumerar rutas de gateway existentes en una malla de servicio	List	virtualGateway*		
ListMeshes	Otorga permiso para enumerar las mallas de servicio existentes	List			
ListRoutes	Otorga permiso para enumerar rutas existentes en una malla de servicio	List	virtualRouter*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso de App Mesh.	List	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListVirtualGateways	Otorga permiso para enumerar gateways virtuales existentes en una malla de servicio	List	mesh*		
ListVirtualNodes	Otorga permiso para enumerar nodos virtuales existentes	List	mesh*		
ListVirtualRouters	Otorga permiso para enumerar enrutadores virtuales existentes en una malla de servicio	List	mesh*		
ListVirtualServices	Otorga permiso para enumerar los servicios virtuales existentes en una malla de servicio	Enumeración	mesh*		
PutMeshPolicy [solo permiso]	Concede permiso para definir la política de una malla de control de acceso a la RAM	Escritura	mesh*		
StreamAggregatedResources	Otorga permiso para recibir recursos transmitidos para un punto final de App Mesh (VirtualNode/VirtualGateway)	Lectura	virtualGateway		
			virtualNode		
TagResource	Otorga permiso para etiquetar un recurso con un recurso especificado	Etiquetado	gatewayRoute		
			mesh		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso	Etiquetado	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			virtualRouter		
			virtualService		
				aws:TagKeys	
UpdateGatewayRoute	Otorga permiso para actualizar una ruta de gateway existente para una malla de servicio especificada y una gateway virtual	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Otorga permiso para actualizar una malla de servicio existente	Write	mesh*		
UpdateRoute	Otorga permiso para actualizar una ruta existente para una malla de servicio especificada y un enrutador virtual	Write	route*		
			virtualNode		
UpdateVirtualGateway	Otorga permiso para actualizar una gateway virtual existente en una malla de servicio especificada	Write	virtualGateway*		
UpdateVirtualNode	Otorga permiso para actualizar un nodo virtual existente en una malla de servicio especificada	Write	virtualNode*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateVirtualRouter	Otorga permiso para actualizar un enrutador virtual existente en una malla de servicio especificada	Write	virtualRouter*		
UpdateVirtualService	Otorga permiso para actualizar un servicio virtual existente en una malla de servicio especificada	Write	virtualService*		
			virtualNode		
			virtualRouter		

Tipos de recursos definidos por AWS App Mesh

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
mesh	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}`	aws:ResourceTag/${TagKey}
virtualService	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
virtualNode	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}	aws:ResourceTag/${TagKey}
virtualRouter	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	aws:ResourceTag/${TagKey}
route	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}	aws:ResourceTag/${TagKey}
virtualGateway	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	aws:ResourceTag/${TagKey}
gatewayRoute	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	aws:ResourceTag/${TagKey}

Claves de condición para AWS App Mesh

AWS App Mesh define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones por pares de clave-valor de etiqueta asociados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de si hay claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS App Mesh Preview

AWS App Mesh Preview (prefijo de servicio:`appmesh-preview`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la previsualización de AWS App Mesh
- Tipos de recursos definidos por la previsualización de AWS App Mesh
- Claves de condición para la previsualización de AWS App Mesh

Acciones definidas por la previsualización de AWS App Mesh

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGatewayRoute	Otorga permiso para crear una ruta de gateway asociada a una gateway virtual	Write	gatewayRoute*		
			virtualService		
CreateMesh	Otorga permiso para crear una malla de servicios	Write	mesh*		
CreateRoute	Otorga permiso para crear una ruta asociada a un enrutador virtual	Write	route*		
			virtualNode		
CreateVirtualGateway	Otorga permiso para crear una gateway virtual dentro de una malla de servicio	Write	virtualGateway*		
CreateVirtualNode	Otorga permiso para crear un nodo virtual dentro de una malla de servicio	Write	virtualNode*		
			virtualService		
CreateVirtualRouter	Otorga permiso para crear un enrutador virtual dentro de una malla de servicio	Write	virtualRouter*		
CreateVirtualService	Otorga permiso para crear un servicio virtual dentro de una malla de servicio	Write	virtualService*		
			virtualNode		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			virtualRouter		
DeleteGatewayRoute	Otorga permiso para eliminar una ruta de gateway existente	Write	gatewayRoute*		
DeleteMesh	Otorga permiso para eliminar una instantánea existente	Escritura	mesh*		
DeleteMeshPolicy [solo permiso]	Concede permiso para eliminar la política de una malla de control de acceso a la RAM	Escritura	mesh*		
DeleteRoute	Concede el permiso para eliminar una ruta existente	Write	route*		
DeleteVirtualGateway	Otorga permiso para eliminar una gateway virtual existente	Write	virtualGateway*		
DeleteVirtualNode	Otorga permiso para eliminar un nodo virtual existente	Write	virtualNode*		
DeleteVirtualRouter	Otorga permiso para eliminar un enrutador virtual existente	Write	virtualRouter*		
DeleteVirtualService	Otorga permiso para eliminar un servicio virtual existente	Write	virtualService*		
DescribeGatewayRoute	Otorga permiso para describir una ruta de gateway existente	Read	gatewayRoute*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMesh	Otorga permiso para describir una malla de servicios existente	Read	mesh*		
DescribeRoute	Otorga permiso para describir una ruta existente	Read	route*		
DescribeVirtualGateway	Otorga permiso para describir una gateway virtual existente	Read	virtualGateway*		
DescribeVirtualNode	Otorga permiso para describir un noto virtual existente	Read	virtualNode*		
DescribeVirtualRouter	Otorga permiso para describir un enrutador virtual existente	Read	virtualRouter*		
DescribeVirtualService	Otorga permiso para describir un servicio virtual existente	Lectura	virtualService*		
GetMeshPolicy [solo permiso]	Concede permiso para leer la política de una malla de control de acceso a la RAM	Lectura	mesh*		
ListGatewayRoutes	Otorga permiso para enumerar rutas de gateway existentes en una malla de servicio	List	virtualGateway*		
ListMeshes	Otorga permiso para enumerar las mallas de servicio existentes	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRoutes	Otorga permiso para enumerar rutas existentes en una malla de servicio	List	virtualRouter*		
ListVirtualGateways	Otorga permiso para enumerar gateways virtuales existentes en una malla de servicio	List	mesh*		
ListVirtualNodes	Otorga permiso para enumerar nodos virtuales existentes	List	mesh*		
ListVirtualRouters	Otorga permiso para enumerar enrutadores virtuales existentes en una malla de servicio	List	mesh*		
ListVirtualServices	Otorga permiso para enumerar los servicios virtuales existentes en una malla de servicio	Enumeración	mesh*		
PutMeshPolicy [solo permiso]	Concede permiso para definir la política de una malla de control de acceso a la RAM	Escritura	mesh*		
StreamAggregatedResources	Otorga permiso para recibir recursos transmitidos para un punto final de App Mesh (VirtualNode/VirtualGateway)	Lectura	virtualGateway		
			virtualNode		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGatewayRoute	Otorga permiso para actualizar una ruta de gateway existente para una malla de servicio especificada y una gateway virtual	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Otorga permiso para actualizar una malla de servicio existente	Write	mesh*		
UpdateRoute	Otorga permiso para actualizar una ruta existente para una malla de servicio especificada y un enrutador virtual	Write	route*		
			virtualNode		
UpdateVirtualGateway	Otorga permiso para actualizar una gateway virtual existente en una malla de servicio especificada	Write	virtualGateway*		
UpdateVirtualNode	Otorga permiso para actualizar un nodo virtual existente en una malla de servicio especificada	Write	virtualNode*		
UpdateVirtualRouter	Otorga permiso para actualizar un enrutador virtual existente en una malla de servicio especificada	Write	virtualRouter*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateVirtualService	Otorga permiso para actualizar un servicio virtual existente en una malla de servicio especificada	Write	virtualService*		
			virtualNode		
			virtualRouter		

Tipos de recursos definidos por la previsualización de AWS App Mesh

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
mesh	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}`	
virtualService	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	
virtualNode	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	

Tipos de recurso	ARN	Claves de condición
virtualRouter	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}`	
route	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}`	
virtualGateway	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}`	
gatewayRoute	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}`	

Claves de condición para la previsualización de AWS App Mesh

App Mesh Preview no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS App Runner

AWS App Runner (prefijo de servicio:`apprunner`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS App Runner
- Tipos de recursos definidos por AWS App Runner
- Claves de condición para AWS App Runner

Acciones definidas por AWS App Runner

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateCustomDomain	Otorga permiso para asociar su propio nombre de dominio con la URL del subdominio de AWS App Runner de su servicio de App Runner	Escritura	service*		
AssociateWebAcl [solo permiso]	Otorga permiso para asociar el servicio a una ACL web de AWS WAF	Escritura	service* webacl*		
CreateAutoScalingConfiguration	Otorga permiso para crear un recurso de configuración de escalado automático de AWS App Runner	Escritura	autoscalingconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnection	Otorga permiso para crear un recurso de conexión de AWS App Runner	Escritura	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateObservabilityConfiguration	Otorga permiso para crear un recurso de configuración de observabilidad de AWS App Runner	Escritura	observabilityconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateService	Otorga permiso para crear un recurso de servicio de AWS App Runner	Escritura	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			vpcconnector		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
CreateVpcConnector	Otorga permiso para crear un recurso de conector de VPC de AWS App Runner	Escritura	vpcconnector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcIngressConnection	Otorga permiso para crear un recurso de AWS App Runner VpcIngressConnection	Escritura	vpcingressconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ServiceArn apprunner:VpcId apprunner:VpcEndpointId	
DeleteAutoScalingConfiguration	Otorga permiso para eliminar un recurso de configuración de escalado automático de AWS App Runner	Escritura	autoscalingconfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConnection	Otorga permiso para eliminar un recurso de conexión de AWS App Runner	Escritura	connection*		
DeleteObservabilityConfiguration	Otorga permiso para eliminar un recurso de configuración de observabilidad de AWS App Runner	Escritura	observabilityconfiguration*		
DeleteService	Otorga permiso para eliminar un recurso de servicio de AWS App Runner	Escritura	service*		
DeleteVpcConnector	Concede permiso para eliminar un recurso de AWS conector de VPC de App Runner	Escritura	vpcconnector*		
DeleteVpcIngressConnection	Otorga permiso para eliminar un recurso de AWS App Runner VpcIngressConnection	Escritura	vpcingressconnection*		
DescribeAutoScalingConfiguration	Otorga permiso para recuperar la descripción de un recurso de configuración de escalado automático de AWS App Runner	Lectura	autoscalingconfiguration*		
DescribeCustomDomains	Otorga permiso para recuperar descripciones de nombres de dominio personalizados asociados a un servicio de AWS App Runner	Lectura	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeObservabilityConfiguration	Otorga permiso para recuperar la descripción de un recurso de configuración de observabilidad de AWS App Runner	Lectura	observabilityconfiguration*		
DescribeOperation	Otorga permiso para recuperar la descripción de una operación que se produjo en un servicio de AWS App Runner	Lectura	service*		
DescribeService	Otorga permiso para recuperar la descripción de un recurso de servicio de AWS App Runner	Lectura	service*		
DescribeVpcConnector	Otorga permiso para recuperar la descripción de un recurso de conector de VPC de AWS App Runner	Lectura	vpcconnector*		
DescribeVpcIngressConnection	Otorga permiso para recuperar la descripción de un recurso de AWS App Runner VpcIngressConnection	Lectura	vpcingressconnection*		
DescribeWebAclForService [solo permiso]	Otorga permiso para obtener la ACL web de AWS WAF asociada a un servicio de AWS App Runner	Lectura	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateCustomDomain	Otorga permiso para desasociar un nombre de dominio personalizado de un servicio de AWS App Runner	Escritura	service*		
DisassociateWebAcl [solo permiso]	Otorga permiso para desasociar el servicio con una ACL web de AWS WAF	Escritura	service*		
ListAssociatedServicesForWebAcl [solo permiso]	Otorga permiso para enumerar los servicios que están asociados a una ACL web de AWS WAF	Enumeración	webacl*		
ListAutoScalingConfigurations	Otorga permiso para recuperar una lista de las configuraciones de escalado automático de AWS App Runner en su Cuenta de AWS	Enumeración			
ListConnections	Otorga permiso para recuperar una lista de las conexiones de AWS App Runner en su Cuenta de AWS	Enumeración			
ListObservabilityConfigurations	Otorga permiso para recuperar una lista de configuraciones de observabilidad de AWS App Runner en su Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOperations	Otorga permiso para recuperar una lista de operaciones que se produjeron en un recurso de servicio de AWS App Runner	Enumeración	service*		
ListServices	Otorga permiso para recuperar una lista de los servicios de AWS App Runner en ejecución en su Cuenta de AWS	Enumeración			
ListServicesForAutoScalingConfiguration	Otorga permiso para recuperar una lista de los AppRunner servicios asociados a una configuración de escalado automático de AWS App Runner en su Cuenta de AWS	Enumeración	autoscalingconfiguration*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas asociadas a un recurso de AWS App Runner	Lectura	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			vpcconnector		
ListVpcConnectors	Concede permiso para recuperar una lista de conectores de VPC de AWS App Runner en su Cuenta de AWS	Enumeración			
ListVpcIngressConnections	Otorga permiso para recuperar una lista de AWS App Runner VpcIngressConnections en su Cuenta de AWS	Enumeración			
PauseService	Otorga permiso para pausar un servicio de AWS App Runner activo	Escritura	service*		
ResumeService	Otorga permiso para reanudar un servicio de AWS App Runner activo	Escritura	service*		
StartDeployment	Otorga permiso para iniciar una implementación manual en un servicio de AWS App Runner	Escritura	service*		
TagResource	Otorga permiso para añadir etiquetas o actualizar los valores de las etiquetas de un recurso de AWS App Runner	Etiquetado	autoscalingconfiguration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de AWS App Runner	Etiquetado	autoscalingconfiguration		
			connection		
			observabilityconfiguration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys	
UpdateDefaultAutoScalingConfiguration	Otorga permiso para actualizar una configuración de escalado automático de AWS App Runner para que sea la predeterminada en su Cuenta de AWS	Escritura	autoscalingconfiguration*		
UpdateService	Otorga permiso para actualizar un recurso de servicio de AWS App Runner	Escritura	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
UpdateVpcIngressConnection	Otorga permiso para actualizar un VpcIngressConnection recurso de AWS App Runner	Escritura	vpcingressconnection*		
				apprunner:VpcId apprunner:VpcEndpointId	

Tipos de recursos definidos por AWS App Runner

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

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

Tipos de recurso	ARN	Claves de condición
vpcingressconnection	arn:${Partition}:apprunner:${Region}:${Account}:vpcingressconnection/${VpcIngressConnectionName}/${VpcIngressConnectionId}	aws:ResourceTag/${TagKey}
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	

Claves de condición para AWS App Runner

AWS App Runner define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
apprunner:AutoScalingConfigurationArn	Filtra el acceso por CreateService y UpdateService las acciones en función del ARN de un recurso asociado AutoScalingConfiguration	ARN
apprunner:ConnectionArn	Filtra el acceso por CreateService y UpdateService las acciones en función del ARN de un recurso de conexión asociado	ARN
apprunner:Observab	Filtra el acceso por CreateService y UpdateService las acciones en función del ARN de un recurso asociado ObservabilityConfiguration	ARN

Claves de condición	Descripción	Tipo
ilityConfiguration Arn		
apprunner :ServiceArn	Filtra el acceso por CreateVpcIngressConnection acción en función del ARN de un recurso de servicio asociado	ARN
apprunner :VpcConne ctorArn	Filtra el acceso por CreateService y UpdateService las acciones en función del ARN de un recurso asociado VpcConnector	ARN
apprunner :VpcEndpointId	Filtra el acceso CreateVpcIngressConnection y las UpdateVpcIngressConnection acciones en función del punto final de la VPC de la solicitud	Cadena
apprunner:VpcId	Filtra el acceso por la VPC de la solicitud CreateVpc IngressConnection y las UpdateVpcIngressConnection acciones en función de ella	Cadena
aws:Reque stTag/${TagKey}	Filtra el acceso mediante acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:Resou rceTag/${ TagKey}	Filtra el acceso mediante acciones en función de pares de clave-valor asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante acciones en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS App Studio

AWS App Studio (prefijo de servicio:`appstudio`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS App Studio
- Tipos de recursos definidos por AWS App Studio
- Claves de condición de AWS App Studio

Acciones definidas por AWS App Studio

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountStatus [solo permiso]	Concede permiso para describir el estado actual de la cuenta	Lectura			
GetEnablementJobStatus [solo permiso]	Concede permiso para obtener el estado de un trabajo de habilitación	Lectura			
StartEnablementJob [solo permiso]	Concede permiso para enviar un trabajo de habilitación	Escritura			
StartRollbackEnabl	Concede permiso para revertir un trabajo de habilitación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ementJob [solo permiso]					
StartTeamDeployment [solo permiso]	Concede permiso para iniciar una implementación de equipo	Escritura			

Tipos de recursos definidos por AWS App Studio

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
instance	`arn:${Partition}:appstudio:${Region}:${Account}:instance/${InstanceId}`	
application	`arn:${Partition}:appstudio:${Region}:${Account}:application/${ApplicationId}`	
connector	`arn:${Partition}:appstudio:${Region}:${Account}:connector/${ConnectionId}`	

Claves de condición de AWS App Studio

App Studio no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las instrucciones de las políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de AWS App2Container

AWS App2Container (prefijo de servicio:`a2c`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS App2Container
- Tipos de recursos definidos por AWS App2Container
- Claves de estado para AWS App2Container

Acciones definidas por AWS App2Container

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetContainerizationJobDetails	Concede permiso para obtener los detalles de todos los trabajos de contenedorización	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeploymentJobDetails	Concede permiso para obtener los detalles de todos los trabajos de implementación	Lectura			
StartContainerizationJob	Concede permiso para comenzar un trabajo de contenedorización	Escritura			
StartDeploymentJob	Concede permiso para comenzar un trabajo de implementación	Escritura			

Tipos de recursos definidos por AWS App2Container

AWS App2Container no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS App2Container, especifique `"Resource": "*"` en su política.

Claves de estado para AWS App2Container

App2Container no tiene claves de contexto específicas de servicios que se puedan usar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS AppConfig

AWS AppConfig (prefijo de servicio:`appconfig`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS AppConfig
- Tipos de recursos definidos por AWS AppConfig
- Claves de condición de AWS AppConfig

Acciones definidas por AWS AppConfig

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Concede permiso para crear una aplicación.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationProfile	Concede permiso para crear un perfil de configuración.	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeploymentStrategy	Concede permiso para crear una estrategia de implementación.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Concede permiso para crear un entorno.	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	Otorga permiso para crear una extensión	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtensionAssociation	Otorga permiso para crear una asociación de extensión	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateHostedConfigurationVersion	Concede permiso para crear una versión de configuración alojada	Write	application*		
			configurationprofile*		
DeleteApplication	Concede permiso para eliminar una aplicación.	Write	application*		
DeleteConfigurationProfile	Concede permiso para eliminar un perfil de configuración.	Write	application*		
			configurationprofile*		
DeleteDeploymentStrategy	Concede permiso para eliminar una estrategia de implementación.	Write	deploymentstrategy*		
DeleteEnvironment	Concede permiso para eliminar un entorno.	Escritura	application*		
			environment*		
DeleteExtension	Otorga permiso para eliminar una extensión	Escritura	extension*		
DeleteExtensionAssociation	Otorga permiso para eliminar una asociación de extensión	Escritura	extensionassociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteHostedConfigurationVersion	Concede permiso para eliminar una versión de configuración alojada	Escritura	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetAccountSettings	Otorga permiso para ver la configuración de toda la cuenta AppConfig	Lectura			
GetApplication	Concede permiso para ver detalles de una aplicación.	Read	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	Concede permiso para ver detalles de una configuración.	Read	application*		
			configurationprofile*		
			environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	Concede permiso para ver detalles de un perfil de configuración.	Read	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
GetDeployment	Concede permiso para ver detalles de una implementación.	Read	application*		
			deployment*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	Concede permiso para ver detalles de una estrategia de implementación.	Read	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEnvironment	Concede permiso para ver detalles de un entorno.	Lectura	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetExtension	Otorga permiso para ver detalles sobre una extensión	Lectura	extension*		
				aws:ResourceTag/${TagKey}	
GetExtensionAssociation	Otorga permiso para ver detalles sobre una asociación de extensión	Lectura	extensionassociation*		
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	Concede permiso para ver detalles sobre una versión de configuración alojada	Lectura	application*		
			configurationprofile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			hostedconfigurationversion*		
GetLatestConfiguration	Concede permiso para recuperar una configuración implementada.	Lectura	configuration*		
				aws:ResourceTag/${TagKey}	
ListApplications	Concede permiso para mostrar las aplicaciones de su cuenta.	List			
ListConfigurationProfiles	Concede permiso para mostrar los perfiles de configuración de una aplicación.	List	application*		
ListDeploymentStrategies	Concede permiso para mostrar las estrategias de implementación de su cuenta.	List			
ListDeployments	Concede permiso para mostrar las implementaciones de un entorno.	List	application*		
			environment*		
ListEnvironments	Concede permiso para mostrar los entornos de una aplicación.	Enumeración	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExtensionAssociations	Otorga permiso para enumerar las asociaciones de extensión en su cuenta	Enumeración			
ListExtensions	Otorga permiso para enumerar las extensiones en su cuenta	Enumeración			
ListHostedConfigurationVersions	Concede permiso para enumerar las versiones de configuración alojadas para un perfil de configuración	List	application*		
			configurationprofile*		
ListTagsForResource	Concede permiso para ver una lista de etiquetas de recurso para un recurso especificado	Lectura	application		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			extensionassociation		
				aws:ResourceTag/${TagKey}	
StartConfigurationSession	Concede permiso para iniciar una sesión de configuración.	Escritura	configuration*		
				aws:ResourceTag/${TagKey}	
StartDeployment	Concede permiso para iniciar una implementación.	Write	application*		
			configurationprofile*		
			deploymentstrategy*		
			environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopDeployment	Concede permiso para detener una implementación	Escritura	application*		
			deployment*		
			environment*		
TagResource	Concede permiso para etiquetar un recurso appconfig .	Etiquetado	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar las etiquetas de un recurso appconfig.	Etiquetado	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateAccountSettings	Otorga permiso para modificar la configuración de toda la cuenta AppConfig	Escritura			
UpdateApplication	Concede permiso para modificar una aplicación.	Write	application*		
				aws:ResourceTag/${TagKey}	
UpdateConfigurationProfile	Concede permiso para modificar un perfil de configuración.	Write	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	Concede permiso para modificar una estrategia de implementación.	Write	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	Concede permiso para modificar un entorno.	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	Otorga permiso para modificar una extensión	Escritura	extension*		
				aws:ResourceTag/${TagKey}	
UpdateExtensionAssociation	Otorga permiso para modificar una asociación de extensión	Escritura	extensionassociation*		
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	Concede permiso para validar una configuración.	Escritura	application*		
			configurationprofile*		

Tipos de recursos definidos por AWS AppConfig

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
environment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
configurationprofile	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}`	aws:ResourceTag/${TagKey}
deploymentstrategy	`arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}`	aws:ResourceTag/${TagKey}
hostedconfigurationversion	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}/hostedconfigurationversion/${VersionNumber}`	
configuration	`arn:${Partition}:appconfig:${Region}:${Account}:application/${Applicatio`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
	`nId}/environment/${EnvironmentId}/configuration/${ConfigurationProfileId}`	
extension	`arn:${Partition}:appconfig:${Region}:${Account}:extension/${ExtensionId}/${ExtensionVersionNumber}`	aws:ResourceTag/${TagKey}
extension association	`arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS AppConfig

AWS AppConfig define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según los valores permitidos para una etiqueta específica.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante un par clave-valor de etiqueta asignado al recurso AWS	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS AppFabric

AWS AppFabric (prefijo de servicio:`appfabric`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS AppFabric
- Tipos de recursos definidos por AWS AppFabric
- Claves de condición de AWS AppFabric

Acciones definidas por AWS AppFabric

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetUserAccessTasks	Concede permiso para iniciar tareas de acceso de usuarios para varios usuarios	Escritura	appbundle*		
ConnectAppAuthorization	Otorga permiso para conectar autorizaciones de aplicaciones	Escritura	appauthorization*		
			appbundle*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAppAuthorization	Otorga permiso para crear autorizaciones de aplicaciones para paquetes de aplicaciones	Escritura	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBundle	Otorga permiso para crear paquetes de aplicaciones en su cuenta	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestion	Otorga permiso para crear ingestiones para paquetes de aplicaciones	Escritura	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestionDestination	Otorga permiso para crear destinos de ingestión para paquetes de aplicaciones	Escritura	appbundle*		
			ingestion*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppAuthorization	Otorga permiso para eliminar autorizaciones de aplicaciones dentro de un paquete de aplicaciones	Escritura	appauthorization*		
			appbundle*		
DeleteAppBundle	Otorga permiso para eliminar paquetes de aplicaciones en su cuenta	Escritura	appbundle*		
DeleteIngestion	Otorga permiso para eliminar ingestiones dentro de un paquete de aplicaciones	Escritura	appbundle*		
			ingestion*		
DeleteIngestionDestination	Concede permiso para eliminar destinos dentro de una ingesta	Escritura	appbundle*		
			ingestion*		
			ingestiondestination*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAppAuthorization	Otorga permiso para ver detalles sobre las autorizaciones de aplicaciones	Lectura	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	
GetAppBundle	Otorga permiso para ver detalles sobre paquetes de aplicaciones	Lectura	appbundle*		
				aws:ResourceTag/${TagKey}	
GetIngestion	Concede permiso para ver detalles de ingestas	Lectura	appbundle*		
			ingestion*		
				aws:ResourceTag/${TagKey}	
GetIngestionDestination	Concede permiso para ver detalles sobre destinos de ingestión	Lectura	appbundle*		
			ingestion*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	
ListAppAuthorizations	Otorga permiso para recuperar una lista de autorizaciones de aplicaciones dentro de un paquete de aplicaciones	Enumeración	appbundle*		
ListAppBundles	Otorga permiso para recuperar una lista de paquetes de aplicaciones en su cuenta	Enumeración			
ListIngestionDestinations	Concede permisos para recuperar una lista de destinos dentro de una ingesta	Enumeración	appbundle*		
			ingestion*		
ListIngestions	Otorga permiso para recuperar una lista de ingestiones dentro de un paquete de aplicaciones	Enumeración	appbundle*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de los recursos AppFabric	Lectura	appauthorization		
			appbundle		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ingestion		
			ingestiondestination		
StartIngestion	Concede permiso para iniciar las ingestas	Escritura	appbundle*		
			ingestion*		
StartUserAccessTasks	Concede permiso para iniciar tareas de acceso de usuarios	Escritura	appbundle*		
StopIngestion	Concede permiso para detener las ingestas	Escritura	appbundle*		
			ingestion*		
TagResource	Otorga permiso para etiquetar AppFabric los recursos	Etiquetado	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para eliminar la etiqueta de AppFabric los recursos	Etiquetado	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys	
UpdateAppAuthorization	Otorga permiso para actualizar las autorizaciones de aplicaciones dentro de los paquetes de aplicaciones	Escritura	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIngestionDestination	Concede permiso para actualizar los destinos dentro de las ingestas	Escritura	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS AppFabric

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
appbundle	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppBundleIdentifier}`	aws:ResourceTag/${TagKey}
appauthorization	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
	`/appauthorization/${AppAuthorization Identifier}`	
ingestion	`arn:${Partition}:appfabric:${Region}: ${Account}:appbundle/${AppbundleId}/ ingestion/${IngestionIdentifier}`	aws:ResourceTag/${ TagKey}
ingestion destination	`arn:${Partition}:appfabric:${Region} :${Account}:appbundle/${AppbundleId} /ingestion/${IngestionIdentifier}/in gestiondestination/${IngestionDestin ationIdentifier}`	aws:ResourceTag/${ TagKey}

Claves de condición de AWS AppFabric

AWS AppFabric define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:Reque stTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:Resou rceTag/${ TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon AppFlow

Amazon AppFlow (prefijo de servicio:`appflow`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon AppFlow
- Tipos de recursos definidos por Amazon AppFlow
- Claves de estado de Amazon AppFlow

Acciones definidas por Amazon AppFlow

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelFlowExecutions	Concede permiso para cancelar las ejecuciones en curso de un flujo de Amazon AppFlow	Escritura	flow*		
CreateConnectorProfile	Otorga permiso para crear un perfil de inicio de sesión para usarlo con Amazon AppFlow Flows	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFlow	Otorga permiso para crear un AppFlow flujo de Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnectorProfile	Otorga permiso para eliminar un perfil de inicio de sesión configurado en Amazon AppFlow	Escritura	connectorprofile*		
DeleteFlow	Otorga permiso para eliminar un AppFlow flujo de Amazon	Escritura	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeConnector	Otorga permiso para describir un conector registrado en Amazon AppFlow	Lectura	connector*		
DescribeConnectorEntity	Otorga permiso para describir todos los campos de un objeto en un perfil de inicio de sesión configurado en Amazon AppFlow	Lectura	connectorprofile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConnectorFields [solo permiso]	Otorga permiso para describir todos los campos de un objeto en un perfil de inicio de sesión configurado en Amazon AppFlow (solo para consolas)	Lectura	connectorprofile*		
DescribeConnectorProfiles	Otorga permiso para describir todos los perfiles de inicio de sesión configurados en Amazon AppFlow	Lectura			
DescribeConnectors	Otorga permiso para describir todos los conectores compatibles con Amazon AppFlow	Lectura			
DescribeFlow	Otorga permiso para describir un flujo específico configurado en Amazon AppFlow	Lectura	flow*		
DescribeFlowExecution [solo permiso]	Otorga permiso para describir todas las ejecuciones de flujos de un flujo configurado en Amazon AppFlow (solo para consolas)	Lectura	flow*		
DescribeFlowExecutionRecords	Otorga permiso para describir todas las ejecuciones de flujos de un flujo configurado en Amazon AppFlow	Lectura	flow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFlows [solo permiso]	Otorga permiso para describir todos los flujos configurados en Amazon AppFlow (solo para consolas)	Lectura			
ListConnectorEntities	Otorga permiso para enumerar todos los objetos de un perfil de inicio de sesión configurado en Amazon AppFlow	Enumeración	connectorprofile*		
ListConnectorFields [solo permiso]	Otorga permiso para enumerar todos los objetos de un perfil de inicio de sesión configurado en Amazon AppFlow (solo para consolas)	Lectura	connectorprofile*		
ListConnectors	Otorga permiso para enumerar todos los conectores compatibles con Amazon AppFlow	Enumeración	connector*		
ListFlows	Otorga permiso para enumerar todos los flujos configurados en Amazon AppFlow	Enumeración	flow*		
ListTagsForResource	Concede permiso para enumerar etiquetas para un flujo	Lectura	flow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterConnector	Otorga permiso para registrar un AppFlow conector de Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
ResetConnectorMetadataCache	Otorga permiso para restablecer los metadatos de las entidades de conector que Amazon AppFlow almacenó en su caché	Escritura	connectorprofile*		
RunFlow [solo permiso]	Otorga permiso para ejecutar un flujo configurado en Amazon AppFlow (solo para consolas)	Escritura	flow*		
StartFlow	Otorga permiso para activar (para flujos programados y activados por eventos) o ejecutar (para flujos bajo demanda) un flujo configurado en Amazon AppFlow	Escritura	flow*		
StopFlow	Otorga permiso para desactivar un flujo programado o activado por un evento configurado en Amazon AppFlow	Escritura	flow*		
TagResource		Etiquetado	connector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para etiquetar un flujo o un conector		flow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UnRegisterConnector	Otorga permiso para anular el registro de un conector en Amazon AppFlow	Escritura	connector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para desetiquetar un flujo o un conector	Etiquetado	connector		
			flow		
				aws:TagKeys	
UpdateConnectorProfile	Otorga permiso para actualizar un perfil de inicio de sesión configurado en Amazon AppFlow	Escritura	connectorprofile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnectorRegistration	Otorga permiso para actualizar un conector registrado configurado en Amazon AppFlow	Escritura	connector*		
UpdateFlow	Otorga permiso para actualizar un flujo configurado en Amazon AppFlow	Escritura	flow*		
UseConnectorProfile [solo permiso]	Otorga permiso para usar un perfil de conector al crear un flujo en Amazon AppFlow	Escritura	connectorprofile*		

Tipos de recursos definidos por Amazon AppFlow

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
connectorprofile	`arn:${Partition}:appflow:${Region}:${Account}:connectorprofile/${ProfileName}`	
flow	`arn:${Partition}:appflow:${Region}:${Account}:flow/${FlowName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
connector	`arn:${Partition}:appflow:${Region}:${Account}:connector/${ConnectorLabel}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon AppFlow

Amazon AppFlow define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon AppIntegrations

Amazon AppIntegrations (prefijo de servicio:`app-integrations`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon AppIntegrations
- Tipos de recursos definidos por Amazon AppIntegrations
- Claves de estado de Amazon AppIntegrations

Acciones definidas por Amazon AppIntegrations

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Concede permiso para crear una nueva Application	Escritura	application*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateApplicationAssociation [solo permiso]	Otorga permiso para crear un ApplicationAssociation	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataIntegration	Otorga permiso para crear una nueva DataIntegration	Escritura	data-integration*		appflow:DeleteFlow appflow:DescribeConnectorProfiles iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant profile:GetDomain profile:GetProfileObjectType s3:GetBucketNotification

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					s3:GetEncryptionConfiguration s3:PutBucketNotification
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataIntegrationAssociation	Otorga permiso para crear un DataIntegrationAssociation	Escritura	data-integration*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:TagResource appflow:UseConnectorProfile profile:CreateSnapshot profile:GetSnapshot

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegrationSchedule	Otorga permiso para crear un programa de integración de datos	Escritura	data-integration*		
CreateEventIntegration	Otorga permiso para crear un nuevo EventIntegration	Escritura	event-integration*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventIntegrationAssociation [solo permiso]	Otorga permiso para crear un EventIntegrationAssociation	Escritura	event-integration*		events:PutRule events:PutTargets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permiso para eliminar una Aplicación	Escritura	application*		
				aws:ResourceTag/${TagKey}	
DeleteApplicationAssociation [solo permiso]	Otorga permiso para eliminar un ApplicationAssociation	Escritura	application-association*		
DeleteDataIntegration	Otorga permiso para eliminar un DataIntegration	Escritura	data-integration*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDataIntegrationAssociation [solo permiso]	Otorga permiso para eliminar un DataIntegrationAssociation	Escritura	data-integration-association*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:StopFlow appflow:TagResource appflow:UseConnectorProfile
DeleteEventIntegration	Otorga permiso para eliminar un EventIntegration	Escritura	event-integration*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEventIntegrationAssociation [solo permiso]	Otorga permiso para eliminar un EventIntegrationAssociation	Escritura	event-integration-association*		events:DeleteRule events:ListTargetsByRule events:RemoveTargets
GetApplication	Concede permiso para ver detalles de Application	Lectura	application*		
				aws:ResourceTag/${TagKey}	
GetDataIntegration	Otorga permiso para ver detalles sobre DataIntegrations	Lectura	data-integration*		
				aws:ResourceTag/${TagKey}	
GetDataIntegrationExecution	Otorga permiso para obtener detalles sobre la ejecución de una integración de datos	Lectura	data-integration*		
GetDataIntegrationSchedule	Otorga permiso para obtener detalles sobre un programa de integración de datos	Lectura	data-integration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEventIntegration	Otorga permiso para ver detalles sobre EventIntegrations	Lectura	event-integration*		
				aws:ResourceTag/${TagKey}	
ListApplicationAssociations	Otorga permiso para publicar ApplicationAssociations	Enumeración			
ListApplications	Concede permiso para enumerar Applications	Enumeración			
ListDataIntegrationAssociations	Otorga permiso para publicar DataIntegrationAssociations	Enumeración			
ListDataIntegrationExecutions	Otorga permiso para enumerar las ejecuciones de integración de datos	Enumeración	data-integration*		
ListDataIntegrationSchedules	Otorga permiso para enumerar los cronogramas de integración de datos	Enumeración	data-integration*		
ListDataIntegrations	Otorga permiso para publicar DataIntegrations	Enumeración			
ListEventIntegrationAssociations	Otorga permiso para publicar EventIntegrationAssociations	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEventIntegrations	Otorga permiso para publicar EventIntegrations	Enumeración			
ListTagsForResource	Otorga permiso a la etiqueta de listas para un AppIntegration recurso de Amazon	Lectura	application		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:ResourceTag/${TagKey}	
StartDataIntegrationExecution	Otorga permiso para iniciar una ejecución de integración de datos	Escritura	data-integration*		profile:CreateSegmentSnapshot profile:CreateSnapshot

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar un AppIntegration recurso de Amazon	Etiquetado	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para desetiquetar un recurso de Amazon AppIntegration	Etiquetado	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApplication	Concede permiso para modificar una Application	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateDataIntegration	Otorga permiso para modificar un DataIntegration	Escritura	data-integration*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationAssociation	Otorga permiso para modificar un DataIntegrationAssociation	Escritura	data-integration-association*		profile:CreateSnapshot profile:GetSnapshot
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationSchedule	Otorga permiso para actualizar un programa de integración de datos	Escritura	data-integration*		
UpdateEventIntegration	Otorga permiso para modificar un EventIntegration	Escritura	event-integration*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon AppIntegrations

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
event-integration	`arn:${Partition}:app-integrations:${Region}:${Account}:event-integration/${EventIntegrationName}`	aws:ResourceTag/${TagKey}
event-integration-association	`arn:${Partition}:app-integrations:${Region}:${Account}:event-integration-association/${EventIntegrationName}/${ResourceId}`	aws:ResourceTag/${TagKey}
data-integration	`arn:${Partition}:app-integrations:${Region}:${Account}:data-integration/${DataIntegrationId}`	aws:ResourceTag/${TagKey}
data-integration-association	`arn:${Partition}:app-integrations:${Region}:${Account}:data-integration-association/${DataIntegrationId}/${ResourceId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:app-integrations:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
application-association	`arn:${Partition}:app-integrations:${Region}:${Account}:application-association/${ApplicationId}/${ApplicationAssociationId}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon AppIntegrations

Amazon AppIntegrations define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Application Auto Scaling

AWS Application Auto Scaling (prefijo de servicio:`application-autoscaling`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Application Auto Scaling
- Tipos de recurso definidos por AWS Application Auto Scaling
- Claves de condición para AWS Application Auto Scaling

Acciones definidas por AWS Application Auto Scaling

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteScalingPolicy	Otorga permiso para eliminar una política de escalado	Escritura	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeleteScheduledAction	Otorga permiso para eliminar una acción programada	Escritura	ScalableTarget*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeregisterScalableTarget	Otorga permiso para anular el registro de un destino escalable	Escritura	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeScalableTargets	Otorga permiso para describir uno o más destinos escalables del espacio de nombres especificado	Lectura			
DescribeScalingActivities	Otorga permiso para describir un conjunto de actividades de escalado o todas las actividades de escalado del espacio de nombres especificado	Lectura			
DescribeScalingPolicies	Otorga permiso para describir un conjunto de políticas de escalado o todas las políticas de escalado del espacio de nombres especificado	Lectura			
DescribeScheduledActions	Otorga permiso para describir un conjunto de acciones programadas o todas las acciones programadas del espacio de nombres especificado	Lectura			
GetPredictiveScalingForecast	Concede permiso para recuperar los datos de pronóstico de una política de escalado predictivo	Enumeración			
ListTagsForResource	Concede permiso para enumerar etiquetas de un destino escalable	Lectura	ScalableTarget*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutScalingPolicy	Otorga permiso para crear y actualizar una política de escalado para un destino escalable	Escritura	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	Otorga permiso para crear y actualizar una política de escalado programada para un destino escalable	Escritura	ScalableTarget*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
RegisterScalableTarget	Otorga permiso para registrar AWS o personalizar recursos como objetivos escalables con Application Auto Scaling y para actualizar los parámetros de configuración utilizados para administrar un objetivo escalable	Escritura	ScalableTarget*		application-autoscaling:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	Concede permiso para etiquetar un destino escalable	Etiquetado	ScalableTarget*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas de un destino escalable	Etiquetado	ScalableTarget*		
				aws:TagKeys	

Tipos de recurso definidos por AWS Application Auto Scaling

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ScalableTarget	`arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Application Auto Scaling

AWS Application Auto Scaling define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
application-autoscaling:scalable-dimension	Filtra el acceso por la dimensión escalable que se incluye en la solicitud	Cadena
application-autoscaling:service-namespace	Filtra el acceso por el espacio de nombres del servicio que se incluye en la solicitud	Cadena
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el servicio AWS Application Cost Profiler

AWS El servicio Application Cost Profiler (prefijo de servicio:`application-cost-profiler`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio AWS Application Cost Profiler
- Tipos de recursos definidos por el servicio AWS Application Cost Profiler
- Claves de condición para el servicio AWS Application Cost Profiler

Acciones definidas por el servicio AWS Application Cost Profiler

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReportDefinition	Otorga permiso para eliminar la configuración con un informe específico de Profiler de costes de aplicaciones, deshabilitando así la generación de informes	Escritura			
GetReportDefinition	Otorga permiso para obtener la configuración con una solicitud de informe de Profiler de costes de aplicación específica	Lectura			
ImportApplicationUsage	Otorga permiso para importar el uso de la aplicación desde S3	Write			
ListReportDefinitions	Otorga permiso para obtener una lista de las diferentes configuraciones de informe del analizador de costes de aplicaciones que han creado	Read			
PutReportDefinition	Otorga permiso para crear configuraciones de informes	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	del analizador de costes de aplicación				
UpdateReportDefinition	Otorga permiso para actualizar una configuración de Application Cost Profiler Service existente	Write			

Tipos de recursos definidos por el servicio AWS Application Cost Profiler

AWS El servicio Application Cost Profiler no admite la especificación de un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso al servicio AWS Application Cost Profiler, especifique `"Resource": "*"` en su política.

Claves de condición para el servicio AWS Application Cost Profiler

Application Cost Profiler no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Application Discovery Arsenal

Application Discovery Arsenal (prefijo de servicio: `arsenal`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas del servicio para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Application Discovery Arsenal
- Tipos de recurso definidos por Application Discovery Arsenal
- Claves de condición para Application Discovery Arsenal

Acciones definidas por Application Discovery Arsenal

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterOnPremisesAgent [solo permiso]	Otorga permiso para registrar los recopiladores de datos AWS proporcionados en el Application Discovery Service	Escritura			

Tipos de recurso definidos por Application Discovery Arsenal

Application Discovery Arsenal no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Application Discovery Arsenal, especifique `"Resource": "*"` en la política.

Claves de condición para Application Discovery Arsenal

Application Discovery Arsenal no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de la política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Application Discovery Service

AWS Application Discovery Service (prefijo de servicio:`discovery`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Application Discovery Service
- Tipos de recursos definidos por AWS Application Discovery Service
- Claves de condición para AWS Application Discovery Service

Acciones definidas por AWS Application Discovery Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateConfigurationItemsToApplication	Otorga permiso a la AssociateConfigurationItemsToApplication API. AssociateConfigurationItemsToApplication asocia uno o más elementos de configuración a una aplicación	Escritura			
BatchDeleteAgents	Otorga permiso a la BatchDeleteAgents API. BatchDele	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	teAgents elimina uno o más agents/data recopiladores asociados a tu cuenta, cada uno identificado por su ID de agente. Si se elimina un recopilador de datos no se eliminan los datos recopilados anteriormente				
BatchDeleteImportData	Otorga permiso a la BatchDeleteImportData API. BatchDeleteImportData elimina una o más tareas de importación de Migration Hub, cada una identificada por su ID de importación. Cada tarea de importación tiene diversos registros, que pueden identificar servidores o aplicaciones.	Escritura			
CreateApplication	Otorga permiso a la CreateApplication API. CreateApplication crea una aplicación con el nombre y la descripción indicados	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTags	Concede permiso a la CreateTags API. CreateTags crea una o más etiquetas para los elementos de configuración. Las etiquetas son metadatos que ayudan a clasificar los activos de TI. Esta API acepta una lista de varios elementos de configuración	Etiquetado			
DeleteApplications	Otorga permiso a la DeleteApplications API. DeleteApplications elimina una lista de aplicaciones y sus asociaciones con los elementos de configuración	Escritura			
DeleteTags	Otorga permiso a la DeleteTags API. DeleteTags elimina la asociación entre los elementos de configuración y una o más etiquetas. Esta API acepta una lista de varios elementos de configuración	Etiquetado		aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAgents	Otorga permiso a la DescribeAgents API. DescribeAgents enumera los agentes o el Conector por ID o enumera todos los agents/Connectors asociados a su usuario si no especificó un ID	Lectura			
DescribeBatchDeleteConfigurationTask	Otorga permiso a la DescribeBatchDeleteConfigurationTask API. DescribeBatchDeleteConfigurationTask devuelve los atributos de una tarea de eliminación por lotes para eliminar un conjunto de elementos de configuración. El identificador de tarea proporcionado debe ser el identificador de tarea recibido del resultado de StartBatchDeleteConfigurationTask	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConfigurations	Otorga permiso a la DescribeConfigurations API. DescribeConfigurations recupera los atributos de una lista de elementos IDs de configuración. Todos los datos proporcionados IDs deben ser para el mismo tipo de activo (servidor, aplicación, proceso o conexión). Los campos de salida son específicos del tipo de activo seleccionado. Por ejemplo, la salida de un elemento de configuración de servidor incluye una lista de atributos del servidor, tales como nombre de host, sistema operativo y número de tarjetas de red	Lectura			
DescribeContinuousExports	Otorga permiso a la DescribeContinuousExports API. DescribeContinuousExports enumera las exportaciones especificadas por el ID. Todas las exportaciones continuas asociadas a su usuario se pueden enumerar si llama DescribeContinuousExports tal cual sin pasar ningún parámetro	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeExportConfigurations	Concede permiso a la DescribeExportConfigurations API. DescribeExportConfigurations recupera el estado de un proceso de exportación determinado. Se puede recuperar el estado de un máximo de 100 procesos	Lectura			
DescribeExportTasks	Concede permiso a la DescribeExportTasks API. DescribeExportTasks recupera el estado de una o más tareas de exportación. Se puede recuperar el estado de hasta 100 tareas de exportación	Lectura			
DescribeImportTasks	Otorga permiso a la DescribeImportTasks API. DescribeImportTasks devuelve una serie de tareas de importación para su usuario, incluida la información de estado, las horas IDs, la URL del objeto Amazon S3 del archivo de importación y más	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeTags	Otorga permiso a la DescribeTags API. DescribeTags recupera una lista de elementos de configuración que están etiquetados con una etiqueta específica. O bien recupera una lista de todas las etiquetas asignadas a un elemento de configuración específico.	Lectura			
DisassociateConfigurationItemsFromApplication	Otorga permiso a la DisassociateConfigurationItemsFromApplication API. DisassociateConfigurationItemsFromApplication disocia uno o más elementos de configuración de una aplicación	Escritura			
ExportConfigurations	Otorga permiso a la ExportConfigurations API. ExportConfigurations exporta todos los datos de configuración detectados a un bucket de Amazon S3 o a una aplicación que le permite ver y evaluar los datos. Los datos incluyen etiquetas y asociaciones de etiquetas, procesos, conexiones, servidores y rendimiento del sistema.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDiscoverySummary	Otorga permiso a la GetDiscoverySummary API. GetDiscoverySummary recupera un breve resumen de los activos descubiertos	Lectura			
GetNetworkConnectionGraph	Concede permiso a la GetNetworkConnectionGraph API. GetNetworkConnectionGraph acepta la lista de entrada de una de las siguientes direcciones IP, identificadores de servidor o identificadores de nodos. Devuelve una lista de nodos y bordes que ayuda al cliente a visualizar el gráfico de conexión de la red. Esta API se utiliza para visualizar la funcionalidad de los gráficos de red en la MigrationHub consola	Lectura			
ListConfigurations	Otorga permiso a la ListConfigurations API. ListConfigurations recupera una lista de elementos de configuración según los criterios que especifique en un filtro. Los criterios de filtro identifican los requisitos de relación	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServerNeighbors	Concede permiso a la ListServerNeighbors API. ListServerNeighbors recupera una lista de servidores que están a un salto de red de un servidor específico	Enumeración			
StartBatchDeleteConfigurationTask	Concede permiso a la StartBatchDeleteConfigurationTask API. StartBatchDeleteConfigurationTask inicia una eliminación asíncrona por lotes de los elementos de configuración. Todo lo suministrado IDs debe ser para el mismo tipo de activo (servidor, aplicación, proceso o conexión). El resultado es un ID de tarea exclusivo que se puede utilizar para comprobar el progreso de las eliminaciones	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartContinuousExport	Otorga permiso a la StartContinuousExport API. StartContinuousExport iniciar el flujo continuo de datos descubiertos por el agente hacia Amazon Athena	Escritura			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole
StartDataCollectionByAgentIds	Concede permiso a la StartDataCollectionByAgentIds API. StartDataCollectionByAgentIds indica a los agentes o conectores especificados que comiencen a recopilar datos	Escritura			
StartExportTask	Concede permiso a la StartExportTask API. StartExportTask exporta los datos de configuración sobre las relaciones y los elementos de configuración detectados a un bucket de S3 en un formato específico	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImportTask	Concede permiso a la StartImportTask API. StartImportTask inicia una tarea de importación. La función de importación de Migration Hub le permite importar detalles de su entorno local directamente AWS sin tener que utilizar las herramientas de Application Discovery Service (ADS), como Discovery Connector o Discovery Agent. Esto ofrece la opción de realizar la evaluación y planificación de la migración directamente a partir de los datos importados, incluyendo la posibilidad de agrupar los dispositivos como aplicaciones y realizar un seguimiento de su estado de migración.	Escritura			discovery:AssociateConfigurationItemsToApplication discovery:CreateApplication discovery:CreateTags discovery:GetDiscoverySummary discovery:ListConfigurations s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopContinuousExport	Otorga permiso a la StopContinuousExport API. StopContinuousExport detiene el flujo continuo de datos descubiertos por el agente hacia Amazon Athena	Escritura			
StopDataCollectionByAgentIds	Concede permiso a la StopDataCollectionByAgentIds API. StopDataCollectionByAgentIds ordena a los agentes o conectores especificados que dejen de recopilar datos	Escritura			
UpdateApplication	Otorga permiso a la UpdateApplication API. UpdateApplication actualiza los metadatos sobre una aplicación	Escritura			

Tipos de recursos definidos por AWS Application Discovery Service

AWS Application Discovery Service no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Application Discovery Service, especifique `"Resource": "*"` en la política.

> **Note**
>
> Para separar el acceso, cree y utilice cuentas independientes AWS .

Claves de condición para AWS Application Discovery Service

AWS Application Discovery Service define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Application Migration Service

AWS El Servicio de migración de aplicaciones (prefijo de servicio:`mgn`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Application Migration Service
- Tipos de recursos definidos por AWS Application Migration Service
- Claves de condición para AWS Application Migration Service

Acciones definidas por AWS Application Migration Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ArchiveApplication	Concede permiso para archivar una aplicación	Escritura	ApplicationResource*		
ArchiveWave	Concede permiso para archivar una onda	Escritura	WaveResource*		
AssociateApplications	Concede permiso para asociar aplicaciones a una onda	Escritura	ApplicationResource*		
			WaveResource*		
AssociateSourceServers	Concede permiso para asociar servidores de origen a una aplicación	Escritura	ApplicationResource*		
			SourceServerResource*		
BatchCreateVolumeSnapshotGroupForMgn [solo permiso]	Concede permiso para crear grupo de instantáneas de volumen	Write	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDeleteSnapshotRequestForMgn [solo permiso]	Concede permiso para eliminar la solicitud de instantáneas por lotes	Write			
ChangeServerLifeCycleState	Concede permiso para cambiar el estado del ciclo de vida del servidor de origen	Escritura	SourceServerResource*		
CreateApplication	Concede permiso para crear una aplicación.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Concede permiso para crear conector	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfigurationTemplate	Concede permiso para lanzar una plantilla de configuración de lanzamiento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNetworkMigrationDefinition	Otorga permiso para crear una definición de migración de red	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicationConfigurationTemplate	Concede permiso para crear la plantilla de configuración de reproducción	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVcenterClientForMgn [solo permiso]	Concede permiso para crear el cliente de vcenter.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWave	Concede permiso para crear una onda	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permiso para eliminar una aplicación.	Escritura	ApplicationResource*		
DeleteConnector	Concede permiso para eliminar un conector	Escritura	ConnectorResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteJob	Concede permiso para eliminar el trabajo	Escritura	JobResource*		
DeleteLaunchConfigurationTemplate	Concede permiso para eliminar una plantilla de configuración de lanzamiento	Escritura	LaunchConfigurationTemplateResource*		
DeleteNetworkMigrationDefinition	Otorga permiso para eliminar una definición de migración de red	Escritura	NetworkMigrationDefinitionResource*		
DeleteReplicationConfigurationTemplate	Concede permiso para eliminar la plantilla de configuración de reproducción	Write	ReplicationConfigurationTemplateResource*		
DeleteSourceServer	Concede permiso para eliminar el servidor de origen	Escritura	SourceServerResource*		
DeleteVcenterClient	Concede permiso para eliminar el cliente de vcenter.	Escritura	VcenterClientResource*		
DeleteWave	Concede permiso para eliminar una onda	Escritura	WaveResource*		
DescribeJobLogItems	Concede permiso para describir elementos de registro de trabajo	Read	JobResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeJobs	Concede permiso para describir trabajos	Enumeración			
DescribeLaunchConfigurationTemplates	Concede permiso para describir la plantilla de configuración de lanzamiento	Enumeración			
DescribeReplicationConfigurationTemplates	Concede permiso para describir la plantilla de configuración de reproducción	List			
DescribeReplicationServerAssociationsForMgn [solo permiso]	Concede permiso para describir asociaciones de servidor de reproducción	Read			
DescribeSnapshotRequestsForMgn [solo permiso]	Concede permiso para describir solicitudes de instantáneas	Read			
DescribeSourceServers	Concede permiso para describir servidores de origen	Enumeración			
DescribeVcenterClients	Concede permiso para describir clientes de vcenter.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateApplications	Concede permiso para desasociar aplicaciones de una onda	Escritura	ApplicationResource*		
			WaveResource*		
DisassociateSourceServers	Concede permiso para desasociar servidores de origen de una aplicación	Escritura	ApplicationResource*		
			SourceServerResource*		
DisconnectFromService	Concede permiso para desconectar el servidor de origen del servicio	Write	SourceServerResource*		
FinalizeCutover	Concede permiso para finalizar la transición	Write	SourceServerResource*		
GetAgentCommandForMgn [solo permiso]	Concede permiso para obtener el comando del agente	Read	SourceServerResource*		
GetAgentConfirmedResumeInfoForMgn [solo permiso]	Concede permiso para obtener información de reanudación confirmada del agente	Read	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAgentInstallationAssetsForMgn [solo permiso]	Concede permiso para obtener activos de instalación del agente	Read			
GetAgentReplicationInfoForMgn [solo permiso]	Concede permiso para obtener información de reproducción del agente	Read	SourceServerResource*		
GetAgentRuntimeConfigurationForMgn [solo permiso]	Concede permiso para obtener la configuración de tiempo de ejecución del agente	Read	SourceServerResource*		
GetAgentSnapshotCreditsForMgn [solo permiso]	Concede permiso para obtener créditos de instantáneas del agente	Read	SourceServerResource*		
GetChannelCommandsForMgn [solo permiso]	Concede permiso para obtener comandos de canal	Read			
GetLaunchConfiguration	Concede permiso para obtener la configuración de lanzamiento	Lectura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetNetworkMigrationDefinition	Otorga permiso para obtener una definición de migración de red	Lectura	NetworkMigrationDefinitionResource*		
GetNetworkMigrationMapperSegmentConstruct	Otorga permiso para obtener una construcción de segmento de mapeador de migración de red	Lectura	NetworkMigrationDefinitionResource*		
GetReplicationConfiguration	Concede permiso para obtener la configuración de reproducción	Lectura	SourceServerResource*		
GetVcenterClientCommandsForMgn [solo permiso]	Concede permiso para obtener comandos del cliente de vcenter.	Lectura	VcenterClientResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InitializeService	Concede permiso para inicializar el servicio	Escritura			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueClientCertificateForMgn [solo permiso]	Concede permiso para emitir un certificado de cliente	Escritura	SourceServerResource		
ListApplications	Concede permiso para enumerar los resúmenes de las aplicaciones	Enumeración			
ListConnectors	Concede permiso para enumerar conectores	Lectura			
ListExportErrors	Concede permiso para enumerar los errores de una tarea de exportación	Enumeración	ExportResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExports	Concede permiso para enumerar tareas de exportación	Enumeración			
ListImportErrors	Concede permiso para enumerar los errores de una tarea de importación	Enumeración	ImportResource*		
ListImports	Concede permiso para enumerar las tareas de importación	Enumeración			
ListManagedAccounts	Concede permiso para enumerar las cuentas administradas	Enumeración			
ListNetworkMigrationAnalyses	Otorga permiso para enumerar los análisis de migración de la red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationAnalysisResults	Otorga permiso para enumerar los resultados de los análisis de migración de la red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerationSegments	Otorga permiso para enumerar los segmentos de generación de código de migración de red	Enumeración	NetworkMigrationDefinitionResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNetworkMigrationCodeGenerations	Otorga permiso para enumerar las generaciones de códigos de migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDefinitions	Otorga permiso para enumerar las definiciones de migración de red	Enumeración			
ListNetworkMigrationDeployedStacks	Otorga permiso para enumerar las pilas implementadas por la migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployedStacksDeletions	Otorga permiso para enumerar las pilas eliminadas implementadas por la migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployments	Otorga permiso para enumerar las implementaciones de migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationExecutions	Otorga permiso para enumerar las ejecuciones de migración de red	Enumeración	NetworkMigrationDefinitionResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNetworkMigrationMapperSegmentConstructs	Otorga permiso para enumerar las construcciones de segmentos del mapeador de migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegments	Otorga permiso para enumerar los segmentos del mapeador de migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappings	Otorga permiso para enumerar las asignaciones de migración de red	Enumeración	NetworkMigrationDefinitionResource*		
ListSourceServerActions	Concede permiso para enumerar los documentos de acción del servidor de origen	Enumeración	SourceServerResource*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
ListTemplateActions	Concede permiso para enumerar documentos de acción de plantillas de configuración de lanzamiento	Enumeración	LaunchConfigurationTemplateResource*		
ListWaves	Concede permiso para enumerar los resúmenes de las ondas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
MarkAsArchived	Concede permiso para marcar el servidor de origen como archivado	Write	SourceServerResource*		
NotifyAgentAuthenticationForMgn [solo permiso]	Concede permiso para notificar la autenticación del agente	Write	SourceServerResource*		
NotifyAgentConnectedForMgn [solo permiso]	Concede permiso para notificar al agente conectado	Write	SourceServerResource*		
NotifyAgentDisconnectedForMgn [solo permiso]	Concede permiso para notificar al agente desconectado	Write	SourceServerResource*		
NotifyAgentReplicationProgressForMgn [solo permiso]	Concede permiso para notificar el progreso de reproducción del agente	Write	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
NotifyVcenterClientStartedForMgn [solo permiso]	Concede permiso para notificar al cliente de vcenter iniciado.	Escritura	VcenterClientResource*		
PauseReplication	Concede permiso para pausar la replicación	Escritura	SourceServerResource*		
PutSourceServerAction	Concede permiso para poner el documento de acción del servidor de origen	Escritura	SourceServerResource*		
PutTemplateAction	Concede permiso para poner el documento de acción de una plantilla de configuración de lanzamiento	Escritura	LaunchConfigurationTemplateResource*		
RegisterAgentForMgn [solo permiso]	Concede permiso para registrar al agente	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveSourceServerAction	Concede permiso para eliminar el documento de acción del servidor de origen	Escritura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveTemplateAction	Concede permiso para eliminar el documento de acción de una plantilla de configuración de lanzamiento	Escritura	LaunchConfigurationTemplateResource*		
ResumeReplication	Concede permiso para reanudar la replicación	Escritura	SourceServerResource*		
RetryDataReplication	Concede permiso para reintentar la reproducción	Write	SourceServerResource*		
SendAgentLogsForMgn [solo permiso]	Concede permiso para enviar registros del agente	Write	SourceServerResource*		
SendAgentMetricsForMgn [solo permiso]	Concede permiso para enviar métricas del agente	Write	SourceServerResource*		
SendChannelCommandResultForMgn [solo permiso]	Concede permiso para enviar el resultado del comando de canal	Write			
SendClientLogsForMgn [solo permiso]	Concede permiso para enviar registros de cliente	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendClientMetricsForMgn [solo permiso]	Concede permiso para enviar métricas de cliente	Escritura			
SendVcenterClientCommandResultForMgn [solo permiso]	Concede permiso para enviar el resultado del comando de cliente de vcenter.	Escritura	VcenterClientResource*		
SendVcenterClientLogsForMgn [solo permiso]	Concede permiso para enviar los registros de cliente de vcenter.	Escritura	VcenterClientResource*		
SendVcenterClientMetricsForMgn [solo permiso]	Concede permiso para enviar métricas de cliente de vcenter.	Escritura	VcenterClientResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCutover	Concede permiso para iniciar la transición.	Escritura	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartExport	Concede permiso para iniciar una tarea de exportación	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeLaunchTemplateVersions mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImport	Concede permiso para crear una tarea de importación	Escritura			ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:ModifyLaunchTemplate mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves mgn:TagResource mgn:UpdateLaunchCo

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					nfiguration s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartNetworkMigrationAnalysis	Otorga permiso para iniciar un análisis de migración de red	Escritura	NetworkMigrationDefinitionResource*		directconnect:DescribeConnections directconnect:DescribeDirectConnectGatewayAssociations directconnect:DescribeDirectConnectGatewayAttachments directconnect:DescribeDirectConnectGateways directconnect:DescribeVirtualGateways directconnect:Desc

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ribeVirtualInterfaces ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DeleteTags ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeManagedPrefixLists

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayV

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					pcAttachments ec2:DescribeTransitGateways ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTablePropagations ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis elasticloadbalancing:DescribeListeners elasticloadbalancing:DescribeLoadBalancerAttributes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					elasticloadbalancing:DescribeLoadBalancers elasticloadbalancing:DescribeRules elasticloadbalancing:DescribeTags elasticloadbalancing:DescribeTargetGroupAttributes elasticloadbalancing:DescribeTargetGroups elasticloadbalancing:Descri

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					beTargetHealth globalaccelerator:ListAccelerators globalaccelerator:ListCustomRoutingAccelerators globalaccelerator:ListCustomRoutingEndpointGroups globalaccelerator:ListCustomRoutingListeners globalaccelerator:ListCustomRoutingP

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ortMappings globalaccelerator:ListEndpointGroups globalaccelerator:ListListeners network-firewall:DescribeFirewall network-firewall:DescribeFirewallPolicy network-firewall:DescribeResourcePolicy network-firewall:DescribeRuleGroup

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					network-firewall:ListFirewallPolicies network-firewall:ListFirewalls network-firewall:ListRuleGroups tiros:CreateQuery tiros:ExtendQuery tiros:GetQueryAnswer tiros:GetQueryExplanation tiros:GetQueryExtensionAccounts

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartNetworkMigrationCodeGeneration	Otorga permiso para iniciar la generación del código de migración de la red	Escritura	NetworkMigrationDefinitionResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartNetworkMigrationDeployedStacksDeletion	Otorga permiso para iniciar la eliminación de las pilas desplegadas por la migración de red	Escritura	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DetachInternetGateway ec2:DetachVolume

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DisableTransitGatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:ModifyInstanceAttribute

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartNetworkMigrationDeployment	Otorga permiso para iniciar un despliegue de migración de red	Escritura	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNatGateway ec2:CreateNetworkAcl ec2:CreateNetworkAclEntry ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:CreateRoute ec2:CreateRouteTable ec2:CreateSecurityGroup ec2:CreateSubnet ec2:CreateTags ec2:CreateTransitGatewayRoute ec2:CreateTransitGatewayRouteTable ec2:CreateTransitGatewayVpcAttachment

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DescribeAccountAttributes ec2:DescribeAddresses ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeEgressOnlyInter

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					netGateways ec2:DescribeHosts ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeLaunch

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					TemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeManagedPrefixLists ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables ec2:DescribeSecurityGroupRules ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayVpcAttachments ec2:DescribeTransitGateways ec2:DescribeVolumes ec2:DescribeVpcEndpointServ

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransitGatewayRouteTableP

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTableAssociations ec2:GetTransitGatewayRouteTablePropagations ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis
StartNetworkMigrationMapping	Otorga permiso para iniciar un mapeo de migración de red	Escritura	NetworkMigrationDefinitionResource*		
StartReplication	Concede permiso para iniciar la replicación	Escritura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartTest	Concede permiso para iniciar la prueba	Escritura	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopReplication	Concede permiso para detener la replicación	Escritura	SourceServerResource*		
TagResource	Concede permiso para asignar una etiqueta de recurso.	Etiquetado	ApplicationResource		
			ConnectorResource		
			ExportResource		
			ImportResource		
			JobResource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:RequestTag/${TagKey} mgn:CreateAction aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TerminateTargetInstances	Concede permiso para terminar instancias de destino	Escritura	SourceServerResource*		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveApplication	Concede permiso para desarchivar una aplicación	Escritura	ApplicationResource*		
UnarchiveWave	Concede permiso para desarchivar una onda	Escritura	WaveResource*		
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	ApplicationResource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ConnectorResource		
			JobResource		
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAgentBacklogForMgn [solo permiso]	Concede permiso para actualizar los pendientes del agente	Write	SourceServerResource*		
UpdateAgentConversionInfoForMgn [solo permiso]	Concede permiso para actualizar la información de conversión del agente	Write	SourceServerResource*		
UpdateAgentReplicationInfoForMgn [solo permiso]	Concede permiso para actualizar la información de reproducción del agente	Write	SourceServerResource*		
UpdateAgentReplicationProcessStateForMgn [solo permiso]	Concede permiso para actualizar el estado del proceso de reproducción del agente	Write	SourceServerResource*		
UpdateAgentSourcePropertiesForMgn [solo permiso]	Concede permiso para actualizar las propiedades de origen del agente	Escritura	SourceServerResource*		
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	ApplicationResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnector	Concede permiso para actualizar el conector	Escritura	ConnectorResource*		
UpdateLaunchConfiguration	Concede permiso para actualizar la configuración de lanzamiento	Escritura	SourceServerResource*		
UpdateLaunchConfigurationTemplate	Concede permiso para actualizar la configuración de lanzamiento	Escritura	LaunchConfigurationTemplateResource*		
UpdateNetworkMigrationDefinition	Otorga permiso para actualizar una definición de migración de red	Escritura	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegment	Otorga permiso para actualizar un segmento del mapeador de migración de red	Escritura	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegmentConstruct	Otorga permiso para actualizar una construcción de segmento del mapeador de migración de red	Escritura	NetworkMigrationDefinitionResource*		
UpdateReplicationConfiguration	Concede permiso para actualizar la configuración de reproducción	Write	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateReplicationConfigurationTemplate	Concede permiso para actualizar la plantilla de configuración de reproducción	Escritura	ReplicationConfigurationTemplateResource*		
UpdateSourceServer	Concede permiso para actualizar el servidor de origen	Escritura	SourceServerResource*		
UpdateSourceServerReplicationType	Concede permiso para actualizar el tipo de replicación de servidor de origen.	Escritura	SourceServerResource*		
UpdateWave	Concede permiso para actualizar una onda	Escritura	WaveResource*		
VerifyClientRoleForMgn [solo permiso]	Concede permiso para verificar el rol de cliente	Lectura			

Tipos de recursos definidos por AWS Application Migration Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
JobResource	arn:${Partition}:mgn:${Region}:${Account}:job/${JobID}	aws:ResourceTag/${TagKey}
ReplicationConfigurationTemplateResource	arn:${Partition}:mgn:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	arn:${Partition}:mgn:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}	aws:ResourceTag/${TagKey}
VcenterClientResource	arn:${Partition}:mgn:${Region}:${Account}:vcenter-client/${VcenterClientID}	aws:ResourceTag/${TagKey}
SourceServerResource	arn:${Partition}:mgn:${Region}:${Account}:source-server/${SourceServerID}	aws:ResourceTag/${TagKey}
ApplicationResource	arn:${Partition}:mgn:${Region}:${Account}:application/${ApplicationID}	aws:ResourceTag/${TagKey}
WaveResource	arn:${Partition}:mgn:${Region}:${Account}:wave/${WaveID}	aws:ResourceTag/${TagKey}
ImportResource	arn:${Partition}:mgn:${Region}:${Account}:import/${ImportID}	aws:ResourceTag/${TagKey}
ExportResource	arn:${Partition}:mgn:${Region}:${Account}:export/${ExportID}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Connector Resource	`arn:${Partition}:mgn:${Region}:${Account}:connector/${ConnectorID}`	aws:ResourceTag/${TagKey}
NetworkMigrationDefinitionResource	`arn:${Partition}:mgn:${Region}:${Account}:network-migration-definition/${NetworkMigrationDefinitionID}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Application Migration Service

AWS El Servicio de migración de aplicaciones define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso según la presencia de claves de etiqueta en la solicitud.	ArrayOfString
mgn:CreateAction	Filtra el acceso mediante el nombre de una acción de API que crea recursos	Cadena

Acciones, recursos y claves de condición de Amazon Application Recovery Controller - Zonal Shift

Amazon Application Recovery Controller: Zonal Shift (prefijo de servicio:`arc-zonal-shift`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Application Recovery Controller - Zonal Shift
- Tipos de recursos definidos por Amazon Application Recovery Controller - Zonal Shift
- Claves de condición para Amazon Application Recovery Controller - Zonal Shift

Acciones definidas por Amazon Application Recovery Controller - Zonal Shift

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelZonalShift	Otorga permiso para cancelar un cambio de zona activo	Escritura	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreatePracticeRunConfiguration	Concede permiso para crear una configuración de ejecución de práctica	Escritura	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeletePracticeRunConfiguration	Concede permiso para eliminar una configuración de ejecución de práctica	Escritura	ALB* NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetAutoshiftObserverNotificationStatus	Concede permiso para obtener el estado de notificación del observador de cambio automático	Lectura			
GetManagedResource	Otorga permiso para obtener información sobre un recurso administrado	Lectura	ALB* NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	Concede permiso para enumerar cambios automáticos activos y completados	Enumeración			
ListManagedResources	Otorga permiso para enumerar los recursos administrados	Enumeración			
ListZonalShifts	Otorga permiso para enumerar los cambios de zona	Enumeración			
StartZonalShift	Otorga permiso para comenzar un cambio de zona	Escritura	ALB*		
			NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateAutoshiftObserverNotificationStatus	Concede permiso para actualizar el estado de notificación del observador de cambio automático	Escritura			
UpdatePracticeRunConfiguration	Concede permiso para actualizar una configuración de ejecución de práctica	Escritura	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalAutoshiftConfiguration	Concede permiso para actualizar a un estado de cambio automático de zonas	Escritura	ALB* NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	Otorga permiso para actualizar un cambio de zona existente	Escritura	ALB*		
			NLB*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon Application Recovery Controller - Zonal Shift

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ALB	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	arc-zonal-shift:ResourceIdentifier

Tipos de recurso	ARN	Claves de condición
		aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
NLB	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}`	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Claves de condición para Amazon Application Recovery Controller - Zonal Shift

Amazon Application Recovery Controller: Zonal Shift define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
arc-zonal-shift:ResourceIdentifier	Filtra el acceso por el identificador de recurso del recurso gestionado	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso administrado	Cadena
elasticloadbalancing:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso administrado	Cadena

Acciones, recursos y claves de condición para AWS Application Transformation Service

AWS El Servicio de transformación de aplicaciones (prefijo de servicio:`application-transformation`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Application Transformation Service
- Tipos de recursos definidos por AWS Application Transformation Service
- Claves de condición para AWS Application Transformation Service

Acciones definidas por AWS Application Transformation Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetContainerization	Concede permiso para obtener los detalles de todos los trabajos de contenedorización	Lectura			
GetDeployment	Concede permiso para obtener los detalles de todos los trabajos de implementación	Lectura			
GetGroupingAssessment	Otorga permiso para obtener los detalles de una operación de evaluación de agrupamiento	Lectura			
GetPortingCompatibilityAssessment	Otorga permiso para obtener una operación de compatibilidad de portabilidad	Lectura			
GetPortingRecommendationAssessment	Otorga permiso para obtener los detalles de una operación de evaluación de las recomendaciones de portabilidad	Lectura			
GetRuntimeAssessment	Otorga permiso para obtener los detalles de una operación de evaluación del tiempo de ejecución	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutLogData	Otorga permiso para enviar registros (destinado únicamente a clientes)	Escritura			
PutMetricData	Otorga permiso para enviar datos de métricas (solo para clientes)	Escritura			
StartContainerization	Concede permiso para comenzar un trabajo de contenedorización	Escritura			
StartDeployment	Concede permiso para comenzar un trabajo de implementación	Escritura			
StartGroupingAssessment	Otorga permiso para iniciar una operación de evaluación de agrupamiento	Escritura			
StartPortingCompatibilityAssessment	Otorga permiso para iniciar una operación de compatibilidad de portabilidad	Escritura			
StartPortingRecommendationAssessment	Otorga permiso para iniciar la operación de evaluación de las recomendaciones de portabilidad	Escritura			
StartRuntimeAssessment	Otorga permiso para iniciar una operación de evaluación del tiempo de ejecución	Escritura			

Tipos de recursos definidos por AWS Application Transformation Service

AWS El servicio de transformación de aplicaciones no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Application Transformation Service, especifique `"Resource": "*"` en la política.

Claves de condición para AWS Application Transformation Service

Application Transformation Service no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de Amazon AppStream 2.0

Amazon AppStream 2.0 (prefijo de servicio:`appstream`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon AppStream 2.0
- Tipos de recursos definidos por Amazon AppStream 2.0
- Claves de estado de Amazon AppStream 2.0

Acciones definidas por Amazon AppStream 2.0

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateAppBlockBuilderAppBlock	Concede permiso para asociar el constructor de bloques de aplicaciones especificado con el bloque de aplicaciones	Escritura	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationFleet	Otorga permiso para asociar la aplicación especificada con la flota	Escritura	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationToEntitlement	Otorga permiso para asociar la aplicación especificada a la concesión de derechos especificada	Escritura	stack*		
AssociateFleet	Otorga permiso para asociar la flota especificada con la pila especificada	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchAssociateUserStack	Otorga permiso para asociar los usuarios especificados con las pilas especificadas. Los usuarios de un grupo de usuarios no pueden asignarse a pilas con flotas que están unidas a un dominio de Active Directory.	Write	stack*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateUserStack	Otorga permiso para desasociar los usuarios especificados de la pilas especificadas	Escritura	stack*		
				aws:ResourceTag/${TagKey}	
CopyImage	Otorga permiso para copiar la imagen especificada en la misma región o en una nueva región dentro de la misma Cuenta de AWS	Escritura	image*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAppBlock	Otorga permiso para crear un bloque de aplicaciones. Los bloques de aplicaciones almacenan los detalles del disco duro virtual que contiene los archivos de la aplicación en un bucket de S3. También almacena el script de configuración con los detalles sobre cómo montar el disco duro virtual. Los bloques de aplicaciones solo se admiten para flotas elásticas.	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilder	Concede permiso para crear un constructor de bloques de aplicaciones. Un constructor de bloques de aplicaciones es una máquina virtual que se utiliza para crear un bloque de aplicaciones	Escritura	app-block-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilderStreamingURL	Concede permiso para crear una URL para iniciar una sesión de streaming de constructor de bloques de aplicaciones	Escritura	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Otorga permiso para crear una aplicación en una cuenta de cliente. Las aplicaciones almacenan los detalles sobre cómo lanzar aplicaciones en instancias de streaming. Esto solo es admitido por flotas elásticas.	Escritura	app-block*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateDirectoryConfig	Otorga permiso para crear un objeto Directory Config en la AppStream versión 2.0. Este objeto incluye la información de configuración necesaria para unir constructores de imágenes y flotas a dominios de Microsoft Active Directory.	Escritura			
CreateEntitlement	Otorga permiso para crear una concesión de derechos para controlar el acceso a las aplicaciones en función de los atributos de usuario	Escritura	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFleet	Otorga permiso para crear una flota. Una flota es un grupo de instancias de streaming desde donde se lanzan y se transmiten aplicaciones a los usuarios.	Write	fleet*		
			image		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilder	Otorga permiso para crear un constructor de imágenes. Un constructor de imágenes es una máquina virtual que se utiliza para crear una imagen.	Write	image*		
			image-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilderStreamingURL	Otorga permiso para crear una URL para iniciar una sesión de streaming de constructor de imágenes	Write	image-builder*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateStack	Otorga permiso para crear una pila para comenzar a transmitir aplicaciones a los usuarios. Una pila se compone de una flota, políticas de acceso de usuarios y configuraciones de almacenamiento asociadas.	Escritura	stack*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamingURL	Otorga permiso para crear una URL temporal para iniciar una sesión de streaming AppStream 2.0 para el usuario especificado. Una URL de streaming permite probar el streaming de la aplicación sin configuración del usuario.	Escritura	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
CreateThemeForStack	Concede permiso para crear un tema de marca personalizado, que puede incluir un logotipo personalizado, enlaces al sitio web y otros elementos de marca para mostrar a los usuarios	Escritura	stack*		
CreateUpdatedImage	Otorga permiso para actualizar una imagen existente en la cuenta de cliente	Escritura	image*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateUsageReportSubscription	Otorga permiso para crear una suscripción de informes de uso. Los informes de uso se generan a diario.	Write			
CreateUser	Otorga permiso para crear un nuevo usuario en el grupo de usuarios	Escritura			
DeleteAppBlock	Otorga permiso para eliminar el bloque de aplicaciones especificado	Escritura	app-block*		
				aws:ResourceTag/${TagKey}	
DeleteAppBlockBuilder	Concede permiso para eliminar el constructor de bloques de aplicaciones especificado y liberar capacidad	Escritura	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApplication	Otorga permiso para eliminar la aplicación especificada	Escritura	application*		
				aws:ResourceTag/${TagKey}	
DeleteDirectoryConfig	Concede permiso para eliminar el objeto Directory Config especificado de la AppStream versión 2.0. Este objeto incluye la información de configuración necesaria para unir constructores de imágenes y flotas a dominios de Microsoft Active Directory.	Escritura			
DeleteEntitlement	Otorga permiso para eliminar la concesión de derechos especificada	Escritura	stack*		
DeleteFleet	Otorga permiso para eliminar la flota especificada	Write	fleet*		
				aws:ResourceTag/${TagKey}	
DeleteImage	Otorga permiso para eliminar la imagen especificada. No se puede eliminar la imagen cuando se está usando.	Write	image*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteImageBuilder	Otorga permiso para eliminar el constructor de imágenes especificado y liberar capacidad	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
DeleteImagePermissions	Otorga permiso para eliminar permisos para la imagen privada especificada	Write	image*		
				aws:ResourceTag/${TagKey}	
DeleteStack	Otorga permiso para eliminar la pila especificada. Una vez que se elimina la pila, el entorno de streaming de la aplicación proporcionado por la pila deja de estar a disposición de los usuarios. Además, se liberan las reservas realizadas para sesiones de streaming de la aplicación para la pila.	Escritura	stack*		
				aws:ResourceTag/${TagKey}	
DeleteThemeForStack	Concede permiso para eliminar un tema de marca personalizado, que puede incluir un logotipo personalizado, enlaces al sitio web y otros elementos de marca para mostrar a los usuarios	Escritura	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUsageReportSubscription	Otorga permiso para desactivar la generación de informes de uso	Write			
DeleteUser	Otorga permiso para eliminar un usuario del grupo de usuarios	Escritura			
DescribeAppBlockBuilderAppBlockAssociations	Concede permiso para recuperar las asociaciones que están asociadas al constructor de bloques de aplicaciones o al bloque de aplicaciones especificados	Lectura	app-block		
			app-block-builder		
DescribeAppBlockBuilders	Concede permiso para recuperar una lista que describe uno o más constructores de bloques de aplicaciones especificados, si se proporcionan los nombres de dichos constructores. De lo contrario, se describen todos los constructores de bloques de aplicaciones de la cuenta	Lectura	app-block-builder		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAppBlocks	Otorga permiso para recuperar una lista que describe uno o varios bloques de aplicaciones especificados, si proporcionan los ARN de los bloques de aplicaciones. De lo contrario, se describen todos los bloques de aplicaciones de la cuenta.	Lectura	app-block		
DescribeApplicationFleetAssociations	Otorga permiso para recuperar las asociaciones que están asociadas a la aplicación o la flota especificada	Lectura	application		
			fleet		
DescribeApplications	Otorga permiso para recuperar una lista que describe una o más aplicaciones especificadas, si se proporcionan los ARN de la aplicación. De lo contrario, se describen todas las aplicaciones de la cuenta.	Lectura	application		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDirectoryConfigs	Otorga permiso para recuperar una lista que describe uno o más objetos de Directory Config específicos para AppStream 2.0, si se proporcionan los nombres de estos objetos. De lo contrario, se describen todos los objetos Directory Config en la cuenta. Este objeto incluye la información de configuración necesaria para unir constructores de imágenes y flotas a dominios de Microsoft Active Directory.	Lectura			
DescribeEntitlements	Otorga permiso para recuperar una o todas las concesiones de derechos para la pila especificada	Lectura	stack*		
DescribeFleets	Otorga permiso para recuperar una lista que describe una o varias flotas especificadas, si proporcionan los nombres de las flotas. De lo contrario, se describen todas las flotas de la cuenta.	Read	fleet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeImageBuilders	Otorga permiso para recuperar una lista que describe uno o más constructores de imágenes especificados, si se proporcionan los nombres de los constructores. De lo contrario, se describen todos los constructores de imágenes de la cuenta.	Lectura	image-builder		
DescribeImagePermissions	Otorga permiso para recuperar una lista que describe los permisos para Cuenta de AWS IDs compartirla en una imagen privada de su propiedad	Lectura	image*		
DescribeImages	Otorga permiso para recuperar una lista que describe una o más imágenes específicas, si se proporcionan los nombres o la imagen de ARNs las imágenes. De lo contrario, se describen todas las imágenes de la cuenta.	Read	image		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSessions	Otorga permiso para recuperar una lista que describe las sesiones de streaming para la flota y pila especificadas. Si se proporciona un ID de usuario para la pila y la flota, solo se describen las sesiones de streaming para ese usuario.	Read	fleet* stack*		
DescribeStacks	Otorga permiso para recuperar una lista que describe una o más pilas especificadas, si se proporcionan los nombres de las pilas. De lo contrario, se describen todas las pilas de la cuenta.	Lectura	stack		
DescribeThemeForStack	Concede permiso para obtener la información del tema de marca personalizada, que puede incluir un logotipo personalizado, enlaces al sitio web y otros elementos de marca para mostrar a los usuarios	Lectura	stack*		
DescribeUsageReportSubscriptions	Otorga permiso para recuperar una lista que describe una o más suscripciones de informes de uso	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeUserStackAssociations	Otorga permiso para recuperar una lista que describe los UserStack Association objetos	Lectura	stack		
DescribeUsers	Otorga permiso para recuperar una lista que describe los usuarios del grupo de usuarios	Read			
DisableUser	Otorga permiso para desactivar el usuario especificado en el grupo de usuarios. Esta acción no elimina el usuario.	Escritura			
DisassociateAppBlockBuilderAppBlock	Concede permiso para desasociar el constructor de bloques de aplicaciones especificado del bloque de aplicaciones	Escritura	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFleet	Otorga permiso para desasociar la aplicación especificada de la flota especificada.	Escritura	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateApplicationFromEntitlement	Otorga permiso para desasociar la aplicación especificada de la concesión de derechos especificada	Escritura	stack*		
DisassociateFleet	Otorga permiso para desasociar la flota especificada de la pila especificada	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
EnableUser	Otorga permiso para habilitar un usuario en el grupo de usuarios	Write			
ExpireSession	Otorga permiso para detener inmediatamente la sesión de streaming especificada	Write			
ListAssociatedFleets	Otorga permiso para recuperar el nombre de la flota que está asociada a la pila especificada	Read	stack*		
ListAssociatedStacks	Otorga permiso para recuperar el nombre de la pila con la que está asociada la flota especificada	Lectura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntitledApplications	Otorga permiso para recuperar las aplicaciones asociadas con la concesión de derechos especificada	Enumeración	stack*		
ListTagsForResource	Otorga permiso para recuperar una lista de todas las etiquetas del recurso AppStream 2.0 especificado. Se pueden etiquetar los siguientes recursos: constructores de imágenes, imágenes, flotas y pilas.	Lectura			
StartAppBlockBuilder	Concede permiso para iniciar el constructor de bloques de aplicaciones especificado	Escritura	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StartFleet	Otorga permiso para iniciar la flota especificada	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StartImageBuilder	Otorga permiso para iniciar el constructor de imágenes especificado	Escritura	image-builder*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
StopAppBlockBuilder	Concede permiso para detener el constructor de bloques de aplicaciones especificado	Escritura	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StopFleet	Otorga permiso para detener la flota especificada	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StopImageBuilder	Otorga permiso para detener el constructor de imágenes especificado	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
Stream	Otorga permiso a los usuarios federados para iniciar sesión con sus credenciales existentes y transmitir aplicaciones desde la pila especificada	Escritura	stack*		
				appstream:userId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar o sobrescribir una o más etiquetas para el recurso AppStream 2.0 especificado. Se pueden etiquetar los siguientes recursos: constructores de imágenes, imágenes, flotas, pilas, bloques de aplicaciones y aplicaciones.	Etiquetado	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para desasociar una o más etiquetas del recurso 2.0 especificado AppStream	Etiquetado	app-block		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:TagKeys	
UpdateAppBlockBuilder	Concede permiso para actualizar un constructor de bloques de aplicaciones especificado. Un constructor de bloques de aplicaciones es una máquina virtual que se utiliza para crear un bloque de aplicaciones	Escritura	app-block-builder*		
				aws:ResourceTag/${TagKey}	
UpdateApplication	Otorga permiso para actualizar los campos especificados en la aplicación especificada	Escritura	application*		
			app-block		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateDirectoryConfig	Concede permiso para actualizar el objeto Directory Config especificado en la AppStream versión 2.0. Este objeto incluye la información de configuración necesaria para unir constructores de imágenes y flotas a dominios de Microsoft Active Directory.	Escritura			
UpdateEntitlement	Otorga permiso para actualizar los campos especificados para la concesión de derechos especificada	Escritura	stack*		
UpdateFleet	Otorga permiso para actualizar la flota especificada. Cuando la flota se encuentra en el estado STOPPED (DETENIDO), se pueden actualizar todos los atributos, excepto el nombre de la flota.	Write	fleet*		
			image		
				aws:ResourceTag/${TagKey}	
UpdateImagePermissions	Otorga permiso para agregar o actualizar permisos en la imagen privada especificada	Write	image*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateStack	Otorga permiso para actualizar los campos especificados en la pila especificada	Escritura	stack*		
				aws:ResourceTag/${TagKey}	
UpdateThemeForStack	Concede permiso para actualizar la información del tema de marca personalizada, que puede incluir un logotipo personalizado, enlaces al sitio web y otros elementos de marca para mostrar a los usuarios	Escritura	stack*		

Tipos de recursos definidos por Amazon AppStream 2.0

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
fleet	`arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
image-builder	`arn:${Partition}:appstream:${Region}:${Account}:image-builder/${ImageBuilderName}`	aws:ResourceTag/${TagKey}
stack	`arn:${Partition}:appstream:${Region}:${Account}:stack/${StackName}`	aws:ResourceTag/${TagKey}
app-block	`arn:${Partition}:appstream:${Region}:${Account}:app-block/${AppBlockName}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:appstream:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
app-block-builder	`arn:${Partition}:appstream:${Region}:${Account}:app-block-builder/${AppBlockBuilderName}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon AppStream 2.0

Amazon AppStream 2.0 define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
appstream:userId	Filtra el acceso por el ID del usuario AppStream 2.0	Cadena

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS AppSync

AWS AppSync (prefijo de servicio:`appsync`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS AppSync
- Tipos de recursos definidos por AWS AppSync
- Claves de condición de AWS AppSync

Acciones definidas por AWS AppSync

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateApi	Otorga permiso para adjuntar una API de GraphQL a un nombre de dominio personalizado en AppSync	Escritura	domain*		
AssociateMergedGraphqlApi	Concede permiso para asociar una API combinada a una API de origen	Escritura	graphqlapi*		
AssociateSourceGraphqlApi	Concede permiso para asociar una API de origen a una API combinada	Escritura	graphqlapi*		
CreateApi	Otorga permiso para crear una API	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateApiCache	Otorga permiso para crear una caché de API en AppSync	Escritura			
CreateApiKey	Otorga permiso para crear una clave única que puede distribuir a los clientes que están ejecutando su API	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateChannelNamespace	Otorga permiso para crear un espacio de nombres de canal	Escritura	channelNamespace*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Concede permiso para crear un origen de datos	Escritura			
CreateDomainName	Otorga permiso para crear un nombre de dominio personalizado en AppSync	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Otorga permiso para crear una nueva función	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGraphqlApi	Otorga permiso para crear una API de GraphQL, que es el recurso de nivel superior AppSync	Escritura		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	Otorga permiso para crear un solucionador. Un solucionador convierte las solicitudes entrantes a un formato que un origen de datos pueda comprender y convierte las respuestas del origen de datos en GraphQL	Escritura			
CreateType	Otorga permiso para crear un nuevo tipo	Escritura			
DeleteApi	Otorga permiso para eliminar una API. Esto también limpiará todos los AppSync recursos que se encuentren debajo de esa API	Escritura	api*		
				aws:ResourceTag/${TagKey}	
DeleteApiCache	Otorga permiso para eliminar la caché de una API en AppSync	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApiKey	Otorga permiso para eliminar una clave API	Escritura			
DeleteChannelNamespace	Otorga permiso para eliminar el espacio de nombres de un canal	Escritura	channelNamespace*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Concede permiso para eliminar un origen de datos	Escritura			
DeleteDomainName	Otorga permiso para eliminar un nombre de dominio personalizado en AppSync	Escritura	domain*		
				aws:ResourceTag/${TagKey}	
DeleteFunction	Otorga permiso para eliminar una función	Escritura			
DeleteGraphqlApi	Otorga permiso para eliminar una API de GraphQL. Esto también limpiará todos los AppSync recursos que estén por debajo de esa API	Escritura	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	Otorga permiso para eliminar un solucionador.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcePolicy [solo permiso]	Concede permiso para eliminar una política de recursos	Escritura			
DeleteType	Otorga permiso para eliminar un tipo	Escritura			
DisassociateApi	Otorga permiso para desvincular una API de GraphQL a un nombre de dominio personalizado en AppSync	Escritura	domain*		
DisassociateMergedGraphqlApi	Concede permiso para eliminar una API de origen asociada de una API combinada identificada por la API de origen	Escritura	mergedApiAssociation*		
DisassociateSourceGraphqlApi	Concede permiso para eliminar una API de origen asociada de una API combinada identificada por la API combinada	Escritura	sourceApiAssociation*		
EvaluateCode	Concede permiso para evaluar código con un tiempo de ejecución y contexto	Lectura			
EvaluateMappingTemplate	Otorga permiso para evaluar la asignación de plantillas	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EventConnect	Otorga permiso para conectarse a una API de eventos	Escritura	api*		
EventPublish	Otorga permiso para publicar eventos en el espacio de nombres de un canal	Escritura	channelNamespace*		
EventSubscribe	Otorga permiso para suscribirse al espacio de nombres de un canal	Escritura	channelNamespace*		
FlushApiCache	Otorga permiso para vaciar la caché de una API AppSync	Escritura			
GetApi	Otorga permiso para recuperar una API	Lectura	api*		
				aws:ResourceTag/${TagKey}	
GetApiAssociation	Otorga permiso para leer los detalles de asociación de la API GraphQL de un nombre de dominio personalizado en AppSync	Lectura	domain*		
GetApiCache	Otorga permiso para leer información sobre la caché de una API en AppSync	Lectura			
GetChannelNamespace	Otorga permiso para recuperar el espacio de nombres de un canal	Lectura	channelNamespace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetDataSource	Otorga permiso para recuperar un origen de datos	Lectura			
GetDataSourceIntrospection	Otorga permiso para recuperar una introspección del origen de datos	Lectura			
GetDomainName	Otorga permiso para leer información sobre un nombre de dominio personalizado en AppSync	Lectura	domain*		
				aws:ResourceTag/${TagKey}	
GetFunction	Otorga permiso para recuperar una función	Lectura			
GetGraphqlApi	Otorga permiso para recuperar una API de GraphQL	Lectura	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	Concede permiso para recuperar las variables de entorno de una API de GraphQL	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIntrospectionSchema	Otorga permisos para recuperar el esquema de introspección para una API de GraphQL	Lectura			
GetResolver	Otorga permiso para recuperar un solucionador	Lectura			
GetResourcePolicy [solo permiso]	Concede permiso para leer una política de recursos	Lectura			
GetSchemaCreationStatus	Otorga permiso para recuperar el estado actual de una operación de creación de esquema	Lectura			
GetSourceApiAssociation	Concede permiso para leer información sobre una API de origen asociada a una API combinada	Lectura	sourceApiAssociation*		
GetType	Otorga permiso para recuperar un tipo	Lectura			
GraphQL [solo permiso]	Otorga permiso para enviar una consulta GraphQL a una API de GraphQL	Escritura	field*		
			graphqlapi*		
ListApiKeys	Otorga permiso para enumerar las claves API de una API determinada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApis	Otorga permiso para publicar APIs	Enumeración		aws:ResourceTag/${TagKey}	
ListChannelNamespaces	Otorga permiso para incluir el espacio de nombres de los canales	Enumeración	api*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Otorga permiso para enumerar los orígenes de datos de una API determinada	Enumeración			
ListDomainNames	Otorga permiso para enumerar nombres de dominio personalizados en AppSync	Enumeración		aws:ResourceTag/${TagKey}	
ListFunctions	Otorga permiso para enumerar las funciones de una API determinada	Enumeración			
ListGraphqlApis	Otorga permiso para publicar GraphQL APIs	Enumeración			
ListResolvers	Otorga permiso para enumerar los solucionadores de una API y un tipo determinados	Enumeración			
ListResolversByFunction	Otorga permiso para enumerar los solucionadores asociados a una función específica	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSourceApiAssociations	Otorga permiso para enumerar la fuente APIs asociada a una API fusionada determinada	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	Otorga permiso para enumerar los tipos de una API determinada	Enumeración			
ListTypesByAssociation	Concede permiso para enumerar los tipos correspondientes a una asociación determinada de API combinada y API de origen	Enumeración			
PutGraphqlApiEnvironmentVariables	Concede permiso para actualizar las variables de entorno de una API de GraphQL	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResourcePolicy [solo permiso]	Concede permiso para establecer una política de recursos	Escritura			
SetWebACL	Otorga permiso para establecer un conjunto de ACL web	Administración de permisos			
SourceGraphQL [solo permiso]	Concede permiso para enviar una consulta GraphQL a una API de origen de una API combinada	Escritura	field* graphqlapi*		
StartDataSourceIntrospection	Concede permiso para hacer una introspección de un origen de datos	Escritura			
StartSchemaCreation	Otorga permiso para agregar un nuevo esquema a la API GraphQL. Esta operación es asíncrona, es decir, GetSchemaCreationStatus puede mostrar cuándo se ha completado	Escritura			
StartSchemaMerge	Concede permiso para iniciar una combinación de esquemas para una API combinada determinada y la API de origen asociada	Escritura	sourceApiAssociation*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	api		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channelNamespace		
			domain		
			graphqlapi		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApi	Otorga permiso para actualizar una API	Escritura	api*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateApiCache	Otorga permiso para actualizar la caché de una API en AppSync	Escritura			
UpdateApiKey	Otorga permiso para actualizar una clave API para una API determinada	Escritura			
UpdateChannelNamespace	Otorga permiso para actualizar el espacio de nombres de un canal	Escritura	channelNamespace*		
				aws:ResourceTag/${TagKey}	
UpdateDataSource	Concede permiso para actualizar un origen de datos	Escritura			
UpdateDomainName	Otorga permiso para actualizar un nombre de dominio personalizado en AppSync	Escritura	domain*		
				aws:ResourceTag/${TagKey}	
UpdateFunction	Otorga permiso para actualizar una función existente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGraphqlApi	Otorga permiso para actualizar una API de GraphQL	Escritura	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	Otorga permiso para actualizar un solucionador.	Escritura			
UpdateSourceApiAssociation	Concede permiso para actualizar una asociación de API combinada y API de origen	Escritura	sourceApiAssociation*		
UpdateType	Otorga permiso para actualizar un tipo	Escritura			

Tipos de recursos definidos por AWS AppSync

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

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

Tipos de recurso	ARN	Claves de condición
channelNamespace	`arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}/channelNamespace/${ChannelNamespaceName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS AppSync

AWS AppSync define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
appsync:Visibility	Filtra el acceso en función de la visibilidad de una API	Cadena
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Artifact

AWS Artifact (prefijo de servicio:`artifact`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Artifact
- Tipos de recursos definidos por AWS Artifact
- Claves de condición para AWS Artifact

Acciones definidas por AWS Artifact

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptAgreement	Otorga permiso para aceptar un AWS acuerdo que la cuenta del cliente aún no ha aceptado	Escritura	agreement*		
AcceptNdaForAgreement	Otorga permiso para aceptar los términos de un documento de confidencialidad para un recurso de acuerdo determinado	Escritura	agreement*		
GetAccountSettings	Concede permiso para obtener la configuración de cuenta de Artifact	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAgreement	Otorga permiso para obtener un AWS acuerdo que la cuenta del cliente aún no ha aceptado	Lectura	agreement*		
GetCustomerAgreement	Otorga permiso para obtener un AWS acuerdo que ha sido aceptado por la cuenta del cliente	Lectura	customer-agreement*		
GetNdaForAgreement	Otorga permiso para recuperar el documento de confidencialidad de un recurso de acuerdo determinado	Lectura	agreement*		
GetReport	Otorga permiso para descargar un informe	Lectura	report*		
GetReportMetadata	Otorga permiso para descargar metadatos asociados a un informe	Lectura	report*		
GetTermForReport	Otorga permiso para descargar un término asociado a un informe	Lectura	report*		
ListAgreements	Otorga permiso para incluir acuerdos AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCustomerAgreements	Otorga permiso para enumerar los recursos del acuerdo con el cliente que han sido aceptados por la cuenta del cliente	Enumeración			
ListReports	Otorga permiso para enumerar los informes de su cuenta	Enumeración			
PutAccountSettings	Concede permiso para establecer la configuración de cuenta de Artifact	Escritura			
TerminateAgreement	Otorga permiso para terminar un contrato de cliente que la cuenta del cliente aceptó previamente	Escritura	customer-agreement*		

Tipos de recursos definidos por AWS Artifact

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
customer-agreement	`arn:${Partition}:artifact::${Account}:customer-agreement/*`	
agreement	`arn:${Partition}:artifact:::agreement/*`	
report	`arn:${Partition}:artifact:${Region}::report/${ReportId}:${Version}`	artifact:ReportCategory artifact:ReportSeries

Claves de condición para AWS Artifact

AWS Artifact define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
artifact:ReportCategory	Filtra el acceso según la categoría a la que están asociados los informes	Cadena
artifact:ReportSeries	Filtra el acceso según la serie a la que están asociados los informes	Cadena

Acciones, recursos y claves de condición para Amazon Athena

Amazon Athena (prefijo de servicio: `athena`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Athena
- Tipos de recurso definidos por Amazon Athena
- Claves de condición de Amazon Athena

Acciones definidas por Amazon Athena

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetNamedQuery	Concede permiso para obtener información acerca de una o varias consultas con nombre	Lectura	workgroup *		
BatchGetPreparedStatement	Otorga permiso para obtener información sobre una o varias instrucciones preparadas	Lectura	workgroup *		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetQueryExecution	Concede permiso para obtener información acerca de una o varias ejecuciones de consultas	Lectura	workgroup*		
CancelCapacityReservation	Concede permiso para cancelar una reserva de capacidad	Escritura	capacity-reservation*		
CancelQueryExecution	Concede permiso para cancelar la ejecución de la consulta. Obsoleto. Se aplica solo a AWS los servicios y principales que utilizan el controlador Athena JDBC anterior a la versión 1.1.0. StopQueryExecution Úselo de otra manera	Escritura	workgroup*		
CreateCapacityReservation	Concede permiso para crear una reserva de capacidad	Escritura	capacity-reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	Concede permiso para crear un catálogo de datos	Escritura	datacatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	Concede permiso para crear una consulta con nombre	Escritura	workgroup*		
CreateNotebook	Otorga permiso para crear un cuaderno	Escritura	workgroup*		
CreatePreparedStatement	Concede permiso para crear una instrucción preparada.	Escritura	workgroup*		
CreatePresignedNotebookUrl	Otorga permiso para crear una URL prefirmada de un cuaderno	Escritura	workgroup*		
CreateWorkGroup	Concede permiso para crear un grupo de trabajo	Escritura	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	Concede permiso para eliminar una reserva de capacidad	Escritura	capacity-reservation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDataCatalog	Concede permiso para eliminar un catálogo de datos	Escritura	datacatalog*		
DeleteNamedQuery	Concede permiso para eliminar una consulta con nombre especificada	Escritura	workgroup*		
DeleteNotebook	Otorga permiso para eliminar un cuaderno	Escritura	workgroup*		
DeletePreparedStatement	Concede permiso para eliminar una instrucción preparada especificada.	Escritura	workgroup*		
DeleteWorkGroup	Concede permiso para eliminar un grupo de trabajo	Escritura	workgroup*		
ExportNotebook	Otorga permiso para exportar un cuaderno	Escritura	workgroup*		
GetCalculationExecution	Otorga permiso para obtener una ejecución de un cálculo	Lectura	workgroup*		
GetCalculationExecutionCode	Otorga permiso para obtener un código de ejecución de un cálculo	Lectura	workgroup*		
GetCalculationExecutionStatus	Otorga permiso para obtener un estado de ejecución de un cálculo	Lectura	workgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCapacityAssignmentConfiguration	Concede permiso para obtener información sobre la asignación de capacidad para una reserva de capacidad	Lectura	capacity-reservation*		
GetCapacityReservation	Concede permiso para obtener una reserva de capacidad	Lectura	capacity-reservation*		
GetCatalogs	Concede permiso para permitir el acceso a bases de datos y tablas. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			
GetDataCatalog	Concede permiso para obtener un catálogo de datos	Lectura	datacatalog*		
GetDatabase	Concede permiso para obtener una base de datos para un determinado catálogo de datos	Lectura	datacatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetExecutionEngine	Concede permiso para permitir el acceso a la base de datos y tabla especificadas. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			
GetExecutionEngines	Concede permiso para permitir el acceso a bases de datos y tablas. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			
GetNamedQuery	Concede permiso para obtener información acerca de una consulta con nombre especificada	Lectura	workgroup *		
GetNamespace	Concede permiso para permitir el acceso a la base de datos y tabla especificadas. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetNamespaces	Concede permiso para permitir el acceso a bases de datos y tablas. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			
GetNotebookMetadata	Otorga permiso para obtener metadatos de un cuaderno	Lectura	workgroup *		
GetPreparedStatement	Concede permiso para obtener información sobre la instrucción preparada especificada	Lectura	workgroup *		
GetQueryExecution	Concede permiso para obtener información sobre la ejecución de consulta especificada	Lectura	workgroup *		
GetQueryExecutions	Concede permiso para ejecuciones de consultas. Obsoleto. Se aplica solo a AWS los servicios y principales que utilizan el controlador Athena JDBC anterior a la versión 1.1.0. ListQueryExecutions Úselo de otra manera	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueryResults	Concede permiso para obtener los resultados de la consulta	Lectura	workgroup*		
GetQueryResultsStream	Concede permiso para obtener el flujo de resultados de la consulta	Lectura	workgroup*		
GetQueryRuntimeStatistics	Otorga permiso para obtener estadísticas de tiempo de ejecución para la ejecución de una consulta especificada	Lectura	workgroup*		
GetSession	Otorga permiso para obtener una sesión	Lectura	workgroup*		
GetSessionStatus	Otorga permiso para obtener el estado de una sesión	Lectura	workgroup*		
GetTable	Concede permiso para permitir el acceso a la tabla especificada. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			
GetTableMetadata	Concede permiso para obtener metadatos sobre una tabla de un catálogo de datos determinado	Lectura	datacatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTables	Concede permiso para permitir el acceso a las tablas. Se aplica únicamente a AWS los servicios gestionados, políticas y principios que utilizan un controlador JDBC de Athena versión 1.1.0	Lectura			
GetWorkGroup	Concede permiso para obtener un grupo de trabajo	Lectura	workgroup *		
ImportNotebook	Otorga permiso para importar un cuaderno	Escritura	workgroup *		
ListApplicationDPUSizes	Otorga permiso para devolver una lista de ApplicationRuntimeIds	Enumeración			
ListCalculationExecutions	Otorga permiso para devolver una lista de ejecuciones de cálculos	Enumeración	workgroup *		
ListCapacityReservations	Otorga permiso para devolver una lista de reservas de capacidad para la capacidad especificada Cuenta de AWS	Enumeración			
ListDataCatalogs	Otorga permiso para devolver una lista de catálogos de datos de la información especificada Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDatabases	Concede permiso para devolver una lista de bases de datos de un catálogo de datos determinado	Enumeración	datacatalog*		
ListEngineVersions	Otorga permiso para devolver una lista de las versiones del motor Athena especificadas Cuenta de AWS	Lectura			
ListExecutors	Otorga permiso para devolver una lista de ejecutores	Enumeración			
ListNamedQueries	Otorga permiso para devolver una lista de consultas con nombre en Amazon Athena para lo especificado Cuenta de AWS	Enumeración	workgroup*		
ListNotebookMetadata	Otorga permiso para devolver una lista de cuadernos de un grupo de trabajo determinado	Enumeración	workgroup*		
ListNotebookSessions	Otorga permiso para devolver una lista de sesiones de un cuaderno determinado	Enumeración	workgroup*		
ListPreparedStatements	Concede permiso para devolver una lista de instrucciones preparadas para el grupo de trabajo especificado.	Enumeración	workgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQueryExecutions	Otorga permiso para devolver una lista de las consultas ejecutadas para la consulta especificada Cuenta de AWS	Lectura	workgroup*		
ListSessions	Otorga permiso para devolver una lista de sesiones de un grupo de trabajo determinado	Enumeración	workgroup*		
ListTableMetadata	Concede permiso para devolver la lista de metadatos de una tabla que se encuentra en una base de datos de un catálogo de datos determinado	Lectura	datacatalog*		
ListTagsForResource	Concede permiso para devolver una lista de etiquetas de un recurso	Lectura	capacity-reservation*		
			datacatalog*		
			workgroup*		
ListWorkGroups	Otorga permiso para devolver una lista de grupos de trabajo para el especificado Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutCapacityAssignmentConfiguration	Concede permiso para asignar capacidad de una reserva de capacidad a consultas	Escritura	capacity-reservation*		
			workgroup*		
RunQuery	Concede permiso para ejecutar una consulta. Obsoleto. Se aplica solo a AWS los servicios y principales que utilizan el controlador Athena JDBC anterior a la versión 1.1.0. StartQueryExecution Úselo de otra manera	Escritura			
StartCalculationExecution	Otorga permiso para iniciar la ejecución de un cálculo	Escritura	workgroup*		
StartQueryExecution	Concede permiso para iniciar una ejecución de consulta mediante una consulta SQL proporcionada como una cadena	Escritura	workgroup*		
StartSession	Otorga permiso para iniciar una sesión	Escritura	workgroup*		
StopCalculationExecution	Otorga permiso para detener la ejecución de un cálculo	Escritura	workgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopQueryExecution	Concede permiso para detener la ejecución de una consulta especificada	Escritura	workgroup*		
TagResource	Otorga permiso para agregar una etiqueta a un recurso.	Etiquetado	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	Otorga permiso para terminar una sesión	Escritura	workgroup*		
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	capacity-reservation*		
			datacatalog*		
			workgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateCapacityReservation	Concede permiso para actualizar una reserva de capacidad	Escritura	capacity-reservation*		
UpdateDataCatalog	Concede permiso para actualizar un catálogo de datos	Escritura	datacatalog*		
UpdateNamedQuery	Concede permiso para actualizar una consulta con nombre especificada	Escritura	workgroup*		
UpdateNotebook	Otorga permiso para actualizar un cuaderno	Escritura	workgroup*		
UpdateNotebookMetadata	Otorga permiso para actualizar metadatos de un cuaderno	Escritura	workgroup*		
UpdatePreparedStatement	Concede permiso para actualizar una instrucción preparada	Escritura	workgroup*		
UpdateWorkGroup	Concede permiso para actualizar un grupo de trabajo	Escritura	workgroup*		

Tipos de recurso definidos por Amazon Athena

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
datacatalog	`arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey}
capacity-reservation	`arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Athena

Amazon Athena define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Audit Manager

AWS Audit Manager (prefijo de servicio:`auditmanager`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Audit Manager
- Tipos de recursos definidos por AWS Audit Manager
- Claves de condición para AWS Audit Manager

Acciones definidas por AWS Audit Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateAssessmentReportEvidenceFolder	Otorga permiso para asociar una carpeta de pruebas a un informe de evaluación en AWS Audit Manager	Escritura	assessment*		
BatchAssociateAssessmentReportEvidence	Otorga permiso para asociar una lista de pruebas a un informe de evaluación en AWS Audit Manager	Escritura	assessment*		
BatchCreateDelegationByAssessment	Otorga permiso para crear delegaciones para una evaluación en AWS Audit Manager	Escritura	assessment*		
			assessmentControlSet*		
BatchDeleteDelegationByAssessment	Otorga permiso para eliminar delegaciones para una evaluación en AWS Audit Manager	Escritura	assessment*		
			assessmentControlSet*		
BatchDisassociateAssessmentReportEvidence	Otorga permiso para desasociar una lista de pruebas de un informe de evaluación en AWS Audit Manager	Escritura	assessment*		
BatchImportEvidenc	Otorga permiso para importar una lista de pruebas a un	Escritura	assessmentControlSet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
eToAssessmentControl	control de evaluación en AWS Audit Manager				
CreateAssessment	Otorga permiso para crear una evaluación para utilizarla con AWS Audit Manager	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentFramework	Otorga permiso para crear un marco para su uso en AWS Audit Manager	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentReport	Otorga permiso para crear un informe de evaluación en AWS Audit Manager	Escritura	assessment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateControl	Otorga permiso para crear un control para su uso en AWS Audit Manager	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAssessment	Otorga permiso para eliminar una evaluación en AWS Audit Manager	Escritura	assessment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFramework	Otorga permiso para eliminar un marco de evaluación en AWS Audit Manager	Escritura	assessmentFramework*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAssessmentFrameworkShare	Otorga permiso para eliminar una solicitud de compartición de un marco personalizado en AWS Audit Manager	Escritura			
DeleteAssessmentReport	Otorga permiso para eliminar un informe de evaluación en AWS Audit Manager	Escritura	assessment*		
DeleteControl	Otorga permiso para eliminar un control en AWS Audit Manager	Escritura	control*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeregisterAccount	Otorga permiso para anular el registro de una cuenta en Audit Manager AWS	Escritura			
DeregisterOrganizationAdminAccount	Otorga permiso para anular el registro de la cuenta de administrador delegado de Audit Manager AWS	Escritura			
DisassociateAssessmentReportEvidenceFolder	Otorga permiso para desasociar una carpeta de pruebas de un informe de evaluación en AWS Audit Manager	Escritura	assessment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountStatus	Otorga permiso para obtener el estado de una cuenta en AWS Audit Manager	Lectura			
GetAssessment	Otorga permiso para crear una evaluación en AWS Audit Manager	Lectura	assessment*		
GetAssessmentFramework	Otorga permiso para obtener un marco de evaluación en AWS Audit Manager	Lectura	assessmentFramework*		
GetAssessmentReportUrl	Otorga permiso para obtener la URL de un informe de evaluación en AWS Audit Manager	Lectura	assessment*		
GetChangeLogs	Otorga permiso para obtener los registros de cambios de una evaluación en Audit Manager AWS	Lectura	assessment*		
GetControl	Otorga permiso para obtener un control en AWS Audit Manager	Lectura	control*		
GetDelegations	Otorga permiso para incluir todas las delegaciones en AWS Audit Manager	Enumeración			
GetEvidence	Otorga permiso para obtener pruebas de AWS Audit Manager	Lectura	assessmentControlSet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEvidenceByEvidenceFolder	Otorga permiso para obtener todas las pruebas de una carpeta de pruebas en AWS Audit Manager	Lectura	assessmentControlSet*		
GetEvidenceFileUploadUrl	Concede permiso para obtener una URL de Amazon S3 prefirmada que se puede utilizar para cargar un archivo como prueba manual	Lectura			
GetEvidenceFolder	Otorga permiso para obtener la carpeta de pruebas de AWS Audit Manager	Lectura	assessmentControlSet*		
GetEvidenceFoldersByAssessment	Otorga permiso para obtener las carpetas de pruebas de una evaluación en AWS Audit Manager	Lectura	assessment*		
GetEvidenceFoldersByAssessmentControl	Otorga permiso para obtener las carpetas de pruebas de un control de evaluación en AWS Audit Manager	Lectura	assessmentControlSet*		
GetInsights	Otorga permiso para obtener datos de análisis para todas las evaluaciones activas.	Lectura			
GetInsightsByAssessment	Otorga permiso para obtener datos de análisis para una evaluación activa específica.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOrganizationAdminAccount	Otorga permiso para obtener la cuenta de administrador delegado en AWS Audit Manager	Lectura			
GetServicesInScope	Otorga permiso para incluir los servicios en el ámbito de una evaluación en AWS Audit Manager	Lectura			
GetSettings	Otorga permiso para configurar todos los ajustes en AWS Audit Manager	Lectura			
ListAssessmentControlInsightsByControlDomain	Otorga permiso para enumerar los datos de análisis para los controles de un dominio de control específico y una evaluación activa.	Enumeración			
ListAssessmentFrameworkShareRequests	Otorga permiso para enumerar todas las solicitudes de compartición enviadas o recibidas para marcos personalizados en AWS Audit Manager	Enumeración			
ListAssessmentFrameworks	Otorga permiso para enumerar todos los marcos de evaluación en AWS Audit Manager	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssessmentReports	Otorga permiso para incluir todos los informes de evaluación en AWS Audit Manager	Enumeración			
ListAssessments	Otorga permiso para enumerar todas las evaluaciones en AWS Audit Manager	Enumeración			
ListControlDomainInsights	Otorga permiso para enumerar los datos de análisis de dominios de control en todas las evaluaciones activas.	Enumeración			
ListControlDomainInsightsByAssessment	Otorga permiso para enumerar los datos de análisis para dominios de control en una evaluación activa específica.	Enumeración			
ListControlInsightsByControlDomain	Otorga permiso para enumerar los datos de análisis para controles de un dominio de control específico en todas las evaluaciones activas.	Enumeración			
ListControls	Otorga permiso para enumerar todos los controles en AWS Audit Manager	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListKeywordsForDataSource	Otorga permiso para enumerar todas las palabras clave de la fuente de datos en AWS Audit Manager	Enumeración			
ListNotifications	Otorga permiso para enumerar todas las notificaciones en AWS Audit Manager	Enumeración			
ListTagsForResource	Otorga permiso para enumerar etiquetas para un recurso AWS de Audit Manager	Lectura	assessment		
			control		
RegisterAccount	Otorga permiso para registrar una cuenta en AWS Audit Manager	Escritura			
RegisterOrganizationAdminAccount	Otorga permiso para registrar una cuenta dentro de la organización como administrador delegado de AWS Audit Manager	Escritura			
StartAssessmentFrameworkShare	Otorga permiso para crear una solicitud de compartición para un marco personalizado en AWS Audit Manager	Escritura	assessmentFramework*		
TagResource	Otorga permiso para etiquetar un recurso AWS de Audit Manager	Etiquetado	assessment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			assessmentFramework		
			control		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para desetiquetar un recurso de AWS Audit Manager	Etiquetado	assessment	aws:ResourceTag/${TagKey}	
			assessmentFramework	aws:ResourceTag/${TagKey}	
			control	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAssessment	Otorga permiso para actualizar una evaluación en AWS Audit Manager	Escritura	assessment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAssessmentControl	Otorga permiso para actualizar un control de evaluación en AWS Audit Manager	Escritura	assessmentControlSet*		
UpdateAssessmentControlSetStatus	Otorga permiso para actualizar el estado de un conjunto de controles de evaluación en AWS Audit Manager	Escritura	assessmentControlSet*		
UpdateAssessmentFramework	Otorga permiso para actualizar un marco de evaluación en AWS Audit Manager	Escritura	assessmentFramework*		
UpdateAssessmentFrameworkShare	Otorga permiso para actualizar una solicitud de compartición de un marco personalizado en AWS Audit Manager	Escritura	assessmentFramework*		
UpdateAssessmentStatus	Otorga permiso para actualizar el estado de una evaluación en AWS Audit Manager	Escritura	assessment*		
UpdateControl	Otorga permiso para actualizar un control en AWS Audit Manager	Escritura	control*		
UpdateSettings	Otorga permiso para actualizar la configuración en AWS Audit Manager	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ValidateAssessmentReportIntegrity	Otorga permiso para validar la integridad de un informe de evaluación en AWS Audit Manager	Lectura			

Tipos de recursos definidos por AWS Audit Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
assessment	`arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}`	aws:ResourceTag/${TagKey}
assessmentFramework	`arn:${Partition}:auditmanager:${Region}:${Account}:assessmentFramework/${AssessmentFrameworkId}`	aws:ResourceTag/${TagKey}
assessmentControlSet	`arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}/controlSet/${ControlSetId}`	
control	`arn:${Partition}:auditmanager:${Region}:${Account}:control/${ControlId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Audit Manager

AWS Audit Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon Aurora DSQL

Amazon Aurora DSQL (prefijo de servicio:`dsql`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Aurora DSQL
- Tipos de recursos definidos por Amazon Aurora DSQL
- Claves de condición de Amazon Aurora DSQL

Acciones definidas por Amazon Aurora DSQL

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddPeerCluster [solo permiso]	Otorga permiso para añadir un clúster homólogo a un clúster multirregional	Escritura	Cluster*		dsql:PutMultiRegionProperties
CreateCluster	Otorga permiso para crear nuevos clústeres	Escritura	Cluster*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys dsql:WitnessRegion	
DbConnect	Otorga permiso para conectarse a la base de datos	Escritura	Cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DbConnectAdmin	Otorga permiso para conectarse a la base de datos con la función de administrador. La conexión con cualquier otro rol requiere DbConnect permiso	Escritura	Cluster*		
DeleteCluster	Otorga permiso para eliminar un clúster y todos sus datos	Escritura	Cluster*		
GetBackupJob	Otorga permiso para obtener el estado de un trabajo de copia de seguridad de un clúster Aurora DSQL	Lectura	Cluster*		
GetCluster	Otorga permiso para obtener información sobre un clúster	Lectura	Cluster*		
GetRestoreJob	Otorga permiso para obtener el estado de un trabajo de restauración de un clúster Aurora DSQL	Lectura	Cluster*		
GetVpcEndpointServiceName	Concede permiso para recuperar el nombre del servicio de punto final de la VPC para un clúster	Lectura	Cluster*		
ListClusters	Otorga permiso para recuperar una lista de clústeres	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas de un recurso DSQL de Aurora	Lectura	Cluster*		
PutMultiRegionProperties [solo permiso]	Otorga permiso para actualizar las propiedades multirregionales de un clúster	Escritura	Cluster*		
PutWitnessRegion [solo permiso]	Otorga permiso para configurar y actualizar la región testigo de un clúster multirregional	Escritura	Cluster*		dsql:PutMultiRegionProperties
				dsql:WitnessRegion	
RemovePeerCluster [solo permiso]	Otorga permiso para eliminar un clúster homólogo de un clúster multirregional	Escritura	Cluster*		dsql:PutMultiRegionProperties
StartBackupJob	Concede permiso para iniciar un trabajo de copia de seguridad para un clúster Aurora DSQL	Escritura	Cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartRestoreJob	Concede permiso para iniciar un trabajo de restauración para un clúster Aurora DSQL	Escritura	Cluster*		dsql:CreateCluster iam:CreateServiceLinkedRole
StopBackupJob	Concede permiso para detener un trabajo de copia de seguridad de un clúster Aurora DSQL	Escritura	Cluster*		
StopRestoreJob	Otorga permiso para detener un trabajo de restauración de un clúster Aurora DSQL	Escritura	Cluster*		
TagResource	Otorga permiso para agregar etiquetas a los recursos de Aurora DSQL	Etiquetado	Cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de los recursos de Aurora DSQL	Etiquetado	Cluster*		
				aws:TagKeys	
UpdateCluster	Otorga permiso para modificar los atributos del clúster	Escritura	Cluster*		
				dsql:WitnessRegion	

Tipos de recursos definidos por Amazon Aurora DSQL

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Cluster	`arn:${Partition}:dsql:${Region}:${Account}:cluster/${Identifier}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Aurora DSQL

Amazon Aurora DSQL define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
dsql:WitnessRegion	Filtra el acceso por región testigo de los clústeres multirregionales	Cadena

Acciones, recursos y claves de condición para AWS Auto Scaling

AWS Auto Scaling (prefijo de servicio:`autoscaling-plans`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Auto Scaling
- Tipos de recursos definidos por AWS Auto Scaling
- Claves de condición para AWS Auto Scaling

Acciones definidas por AWS Auto Scaling

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateScalingPlan	Crea un plan de escalado.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteScalingPlan	Elimina el plan de escalado especificado.	Write			
DescribeScalingPlanResources	Describe los recursos escalables del plan de escalado especificado.	Read			
DescribeScalingPlans	Describe los planes de escalado especificados o todos sus planes de escalado.	Read			
GetScalingPlanResourceForecastData	Recupera los datos de previsión de un recurso escalable.	Read			
UpdateScalingPlan	Actualiza un plan de escalado.	Write			

Tipos de recursos definidos por AWS Auto Scaling

AWS Auto Scaling no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Auto Scaling, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Auto Scaling

Auto Scaling no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el intercambio de datos B2B de AWS

AWS El intercambio de datos B2B (prefijo de servicio:`b2bi`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el intercambio de datos de B2B de AWS
- Tipos de recursos definidos por el intercambio de datos B2B de AWS
- Claves de condición para el intercambio de datos B2B de AWS

Acciones definidas por el intercambio de datos de B2B de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCapability	Concede el permiso para crear una capacidad	Escritura	transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePartnership	Concede permiso para crear una asociación	Escritura	capability*		
			profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile	Otorga permiso para crear un perfil	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateStarterMappingTemplate	Otorga permiso para generar una plantilla de inicio JSONATA/XSLT	Escritura	transformer*		
CreateTransformer	Concede permiso para crear un transformador	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCapability	Concede el permiso para eliminar una capacidad	Escritura	capability*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePartnership	Otorga permiso para eliminar una asociación	Escritura	partnership*		
DeleteProfile	Concede permiso para eliminar un perfil	Escritura	profile*		
DeleteTransformer	Concede permiso para eliminar un transformador	Escritura	transformer*		
GenerateMapping	Otorga permiso para generar una plantilla de JSONATA/XSLT mapeo inicial desde Amazon Bedrock	Escritura	transformer*		
GetCapability	Otorga permiso para obtener una capacidad	Lectura	capability*		
GetPartnership	Concede permiso para obtener una asociación	Lectura	partnership*		
GetProfile	Otorga permiso para obtener un perfil.	Lectura	profile*		
GetTransformer	Concede permiso para obtener un transformador	Lectura	transformer*		
GetTransformerJob	Concede permiso para obtener un trabajo de transformador	Lectura	transformer*		
ListCapabilities	Concede permiso para enumerar todas las capacidades	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPartnerships	Concede permiso para enumerar todas las asociaciones	Enumeración			
ListProfiles	Concede permiso para enumerar todos los perfiles	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso B2Bi	Lectura	capability		
			partnership		
			profile		
			transformer		
ListTransformers	Concede permiso para enumerar todos los transformadores	Enumeración			
StartTransformerJob	Concede permiso al transformador para un documento	Escritura	transformer*		
TagResource	Concede permiso para etiquetar un recurso B2Bi	Etiquetado	capability		
			partnership		
			profile		
			transformer		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConversion	Otorga permiso para convertir un documento JSON/XML en un documento editable	Escritura	transformer*		
TestMapping	Otorga permiso para mapear un archivo de muestra	Escritura	transformer*		
TestParsing	Otorga permiso para analizar un documento edi	Escritura	transformer*		
UntagResource	Concede permiso para eliminar etiquetas en un recurso B2Bi	Etiquetado	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys	
UpdateCapability	Concede el permiso para actualizar una capacidad	Escritura	capability*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			transformer		
UpdatePartnership	Concede el permiso para actualizar una asociación	Escritura	partnership*		
			capability		
UpdateProfile	Otorga permiso para actualizar un perfil.	Escritura	profile*		
UpdateTransformer	Concede permiso para actualizar un transformador	Escritura	transformer*		

Tipos de recursos definidos por el intercambio de datos B2B de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
profile	`arn:${Partition}:b2bi:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
capability	`arn:${Partition}:b2bi:${Region}:${Account}:capability/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
partnership	`arn:${Partition}:b2bi:${Region}:${Account}:partnership/${ResourceId}`	aws:ResourceTag/${TagKey}
transformer	`arn:${Partition}:b2bi:${Region}:${Account}:transformer/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para el intercambio de datos B2B de AWS

AWS El intercambio de datos B2B define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Backup

AWS Backup (prefijo de servicio:`backup`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Backup
- Tipos de recursos definidos por AWS Backup
- Claves de condición para AWS Backup

Acciones definidas por AWS Backup

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateBackupVaultMpaApprovalTeam	Otorga permiso para asociar un equipo de aprobación de la MPA a una bóveda de respaldo	Escritura	backupVault*		
				backup:MpaApprovalTeamArn	
CancelLegalHold	Concede permiso para cancelar una retención legal	Escritura	legalHold*		
CopyFromBackupVault [solo permiso]	Concede permiso para copiar desde un almacén de copia de seguridad.	Write	recoveryPoint*		
				backup:CopyTargets	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				backup:CopyTargetOrgPaths	
CopyIntoBackupVault [solo permiso]	Concede permiso para copiar en un almacén de copia de seguridad.	Write	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupPlan	Concede permiso para crear un nuevo plan de copia de seguridad.	Write	backupPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackupSelection	Concede permiso para crear una nueva asignación de recursos en un plan de copia de seguridad.	Write	backupPlan*		iam:PassRole
CreateBackupVault	Concede permiso para crear un nuevo almacén de copia de seguridad.	Escritura	backupVault*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFramework	Concede permiso para crear un nuevo marco	Escritura	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	Concede permiso para crear una nueva retención legal	Escritura	legalHold*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLogicallyAirGappedBackupVault	Concede permiso para crear un nuevo almacén de copias de seguridad independiente lógicamente, un contenedor lógico donde se almacenan las copias de seguridad	Escritura	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	Concede permiso para crear un nuevo plan de informes	Escritura	reportPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRestoreAccessBackupVault	Otorga permiso para crear un almacén de copias de seguridad con acceso de restauración	Escritura	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingPlan	Concede permiso para crear un nuevo plan de pruebas de restauración	Escritura	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingSelection	Concede permiso para crear una nueva asignación de recursos en un plan de pruebas de restauración	Escritura	restoreTestingPlan*		iam:PassRole
DeleteBackupPlan	Concede permiso para eliminar un plan de copia de seguridad.	Write	backupPlan*		
DeleteBackupSelection	Concede permiso para eliminar una asignación de recursos a partir de un plan de copia de seguridad.	Write	backupPlan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBackupVault	Concede permiso para eliminar un almacén de copia de seguridad.	Write	backupVault*		
DeleteBackupVaultAccessPolicy	Concede permiso para eliminar la política de acceso al almacén de copia de seguridad.	Administración de permisos	backupVault*		
DeleteBackupVaultLockConfiguration	Concede permiso para quitar la configuración de bloqueo de un almacén de copia de seguridad	Escritura	backupVault*		
DeleteBackupVaultNotifications	Concede permiso para quitar notificaciones del almacén de copia de seguridad	Escritura	backupVault*		
DeleteBackupVaultSharingPolicy [solo permiso]	Concede permiso para eliminar la política para compartir del almacén de copia de seguridad	Administración de permisos	backupVault*		
DeleteFramework	Concede permiso para eliminar un marco	Escritura	framework*		
DeleteRecoveryPoint	Concede permiso para eliminar un punto de recuperación de un almacén de copia de seguridad.	Escritura	recoveryPoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReportPlan	Concede permiso para eliminar un plan de informes	Escritura	reportPlan*		
DeleteRestoreTestingPlan	Concede permiso para eliminar un plan de pruebas de restauración	Escritura	restoreTestingPlan*		
DeleteRestoreTestingSelection	Concede permiso para eliminar una asignación de recursos a partir de un plan de pruebas de restauración	Escritura	restoreTestingPlan*		
DescribeBackupJob	Concede permiso para describir un trabajo de copia de seguridad.	Read			
DescribeBackupVault	Concede permiso para describir un nuevo almacén de copia de seguridad con el nombre especificado.	Read	backupVault*		
DescribeCopyJob	Concede permiso para describir un trabajo de copia.	Lectura			
DescribeFramework	Concede permiso para describir un marco con el nombre especificado	Lectura	framework*		
DescribeGlobalSettings	Concede permiso para describir la configuración global.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeProtectedResource	Concede permiso para describir un recurso protegido.	Read			
DescribeRecoveryPoint	Concede permiso para describir un punto de recuperación.	Read	recoveryPoint*		
DescribeRegionSettings	Concede permiso para describir la configuración de la región.	Lectura			
DescribeReportJob	Concede permiso para describir un trabajo de informes	Lectura			
DescribeReportPlan	Concede permiso para describir un plan de informes con el nombre especificado	Lectura	reportPlan*		
DescribeRestoreJob	Concede permiso para describir un trabajo de restauración.	Lectura			
DisassociateBackupVaultMpaApprovalTeam	Otorga permiso para desvincular a un equipo de aprobación de la MPA de una bóveda de respaldo	Escritura	backupVault*		
DisassociateRecoveryPoint	Concede permiso para desasociar un punto de recuperación de un almacén de copia de seguridad.	Escritura	recoveryPoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateRecoveryPointFromParent	Concede permiso para desasociar un punto de recuperación de su elemento principal	Escritura	recoveryPoint*		
ExportBackupPlanTemplate	Concede permiso para exportar un plan de copia de seguridad como un JSON.	Read			
GetBackupPlan	Concede permiso para obtener un plan de copia de seguridad.	Read	backupPlan*		
GetBackupPlanFromJSON	Concede permiso para transformar un JSON en un plan de copia de seguridad.	Read			
GetBackupPlanFromTemplate	Concede permiso para transformar una plantilla en un plan de copia de seguridad.	Read			
GetBackupSelection	Concede permiso para obtener una asignación de recursos para el plan de copia de seguridad.	Read	backupPlan*		
GetBackupVaultAccessPolicy	Concede permiso para obtener la política de acceso al almacén de copia de seguridad.	Read	backupVault*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBackupVaultNotifications	Concede permiso para obtener notificaciones de almacén de copia de seguridad.	Lectura	backupVault*		
GetBackupVaultSharingPolicy [solo permiso]	Concede permiso para obtener la política para compartir del almacén de copia de seguridad	Lectura	backupVault*		
GetLegalHold	Concede permiso para obtener una retención legal	Lectura	legalHold*		
GetRecoveryPointIndexDetails	Otorga permiso para obtener los detalles de indexación de un punto de recuperación	Lectura	recoveryPoint*		
GetRecoveryPointRestoreMetadata	Concede permiso para obtener metadatos de restauración del punto de recuperación.	Lectura	recoveryPoint*		
GetRestoreJobMetadata	Concede permiso para obtener los metadatos de restauración asociados a un trabajo de restauración	Lectura			
GetRestoreTestingInferredMetadata	Otorga permiso para obtener los metadatos inferidos generados por las pruebas de restauración	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRestoreTestingPlan	Otorga permiso para obtener un plan de pruebas de restauración	Lectura	restoreTestingPlan*		
GetRestoreTestingSelection	Concede permiso para obtener una asignación de recursos para el plan de pruebas de restauración	Lectura	restoreTestingPlan*		
GetSupportedResourceTypes	Concede permiso para obtener tipos de recursos compatibles.	Lectura			
ListBackupJobSummaries	Concede permiso para enumerar resúmenes de trabajos de copia de seguridad	Enumeración			
ListBackupJobs	Concede permiso para enumerar los trabajos de copia de seguridad.	Enumeración			
ListBackupPlanTemplates	Otorga permiso para enumerar las plantillas de planes de respaldo proporcionadas por AWS Backup	Enumeración			
ListBackupPlanVersions	Concede permiso para enumerar versiones del plan de copia de seguridad.	Enumeración	backupPlan*		
ListBackupPlans	Concede permiso para enumerar planes de copia de seguridad.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBackupSelections	Concede permiso para enumerar asignaciones de recursos para un plan de copia de seguridad específico.	Enumeración	backupPlan*		
ListBackupVaults	Concede permiso para enumerar los almacenes de copia de seguridad	Enumeración			
ListCopyJobSummaries	Concede permiso para enumerar los resúmenes de trabajos de copia	Enumeración			
ListCopyJobs	Concede permiso para enumerar trabajos de copia.	Enumeración			
ListFrameworks	Concede permiso para enumerar marcos	Enumeración			
ListIndexedRecoveryPoints	Otorga permiso para obtener puntos de recuperación indexados en la lista	Enumeración			
ListIndexedRecoveryPointsForSearch [solo permiso]	Otorga permiso para enumerar los puntos de recuperación indexados para su búsqueda	Administración de permisos			
ListLegalHolds	Concede permiso para enumerar retenciones legales	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProtectedResources	Concede permiso a AWS Backup para enumerar los recursos protegidos	Enumeración			
ListProtectedResourcesByBackupVault	Concede permiso para enumerar recursos protegidos dentro de un almacén de copias de seguridad	Enumeración	backupVault*		
ListRecoveryPointsByBackupVault	Concede permiso para enumerar los puntos de recuperación dentro de un almacén de copia de seguridad.	Enumeración	backupVault*		
ListRecoveryPointsByLegalHold	Concede permiso para enumerar los puntos de recuperación por retención legal	Enumeración	legalHold*		
ListRecoveryPointsByResource	Concede permiso para enumerar los puntos de recuperación de un recurso.	Enumeración			
ListReportJobs	Concede permiso para enumerar trabajos de informes	Enumeración			
ListReportPlans	Concede permiso para enumerar planes de informes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRestoreAccessBackupVaults	Otorga permiso para enumerar una restauración y acceder a las bóvedas de respaldo asociadas a una bóveda de respaldo	Enumeración	backupVault*		
ListRestoreJobSummaries	Concede permiso para enumerar los resúmenes de restauración	Enumeración			
ListRestoreJobs	Concede permiso para enumerar trabajos de restauración	Enumeración			
ListRestoreJobsByProtectedResource	Concede permiso para enumerar los trabajos de restauración de un recurso protegido	Enumeración			
ListRestoreTestingPlans	Concede permiso para enumerar planes de pruebas de restauración	Enumeración			
ListRestoreTestingSelections	Concede permiso para enumerar asignaciones de recursos para un plan de pruebas de restauración	Enumeración	restoreTestingPlan*		
ListTags	Concede permiso para enumerar las etiquetas de un recurso	Read	backupPlan		
			backupVault		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
PutBackupVaultAccessPolicy	Concede permiso para agregar una política de acceso al almacén de copia de seguridad.	Administración de permisos	backupVault*		
PutBackupVaultLockConfiguration	Concede permiso para agregar la configuración de bloqueo en un almacén de copia de seguridad	Escritura	backupVault*		
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutBackupVaultNotifications	Concede permiso para agregar un tema SNS al almacén de copia de seguridad.	Escritura	backupVault*		
PutBackupVaultSharingPolicy [solo permiso]	Concede permiso para agregar una política para compartir al almacén de copia de seguridad	Administración de permisos	backupVault*		
PutRestoreValidationResult	Concede permiso para colocar un resultado de validación de restauración	Escritura			
RevokeRestoreAccessBackupVault	Otorga permiso para revocar un almacén de copias de seguridad con acceso de restauración	Escritura	backupVault*		
SearchRecoveryPoint [solo permiso]	Otorga permiso para buscar un punto de recuperación	Administración de permisos	recoveryPoint*		
StartBackupJob	Concede permiso para iniciar un nuevo trabajo de copia de seguridad.	Write	backupVault*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCopyJob	Concede permiso para copiar una copia de seguridad a partir de un almacén de copia de seguridad de origen a un almacén de copia de seguridad de destino.	Escritura	recoveryPoint*		iam:PassRole
StartReportJob	Concede permiso para iniciar un nuevo trabajo de informes	Escritura	reportPlan*		
StartRestoreJob	Concede permiso para iniciar un nuevo trabajo de restauración.	Write	recoveryPoint*		iam:PassRole
StopBackupJob	Concede permiso para detener un trabajo de copia de seguridad.	Write			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			restoreTestingPlan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateBackupPlan	Concede permiso para actualizar un plan de copia de seguridad.	Escritura	backupPlan*		
UpdateFramework	Concede permiso para actualizar un marco	Escritura	framework*		
UpdateGlobalSettings	Otorga permiso para actualizar la configuración global actual de la AWS cuenta	Escritura			
UpdateRecoveryPointIndexSettings	Otorga permiso para actualizar la configuración del índice de puntos de recuperación	Escritura	recoveryPoint*		
				backup:Index	
UpdateRecoveryPointLifecycle	Concede permiso para actualizar el ciclo de vida del punto de recuperación.	Write	recoveryPoint*		
UpdateRegionSettings	Concede permiso para actualizar la configuración actual de suscripción de servicio para la región.	Escritura			
UpdateReportPlan	Concede permiso para actualizar un plan de informe	Escritura	reportPlan*		
				backup:FrameworkArns	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRestoreTestingPlan	Concede permiso para actualizar un plan de pruebas de restauración	Escritura	restoreTestingPlan *		
UpdateRestoreTestingSelection	Concede permiso para crear una nueva asignación de recursos en un plan de pruebas de restauración	Escritura	restoreTestingPlan *		iam:PassRole

Tipos de recursos definidos por AWS Backup

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
backupVault	`arn:${Partition}:backup:${Region}:${Account}:backup-vault:${BackupVaultName}`	aws:ResourceTag/${TagKey}
backupPlan	`arn:${Partition}:backup:${Region}:${Account}:backup-plan:${BackupPlanId}`	aws:ResourceTag/${TagKey}
recoveryPoint	`arn:${Partition}:${Vendor}:${Region}:*:${ResourceType}:${RecoveryPointId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
framework	`arn:${Partition}:backup:${Region}:${Account}:framework:${FrameworkName}-${FrameworkId}`	aws:ResourceTag/${TagKey}
reportPlan	`arn:${Partition}:backup:${Region}:${Account}:report-plan:${ReportPlanName}-${ReportPlanId}`	aws:ResourceTag/${TagKey}
legalHold	`arn:${Partition}:backup:${Region}:${Account}:legal-hold:${LegalHoldId}`	aws:ResourceTag/${TagKey}
restoreTestingPlan	`arn:${Partition}:backup:${Region}:${Account}:restore-testing-plan:${RestoreTestingPlanName}-${RestoreTestingPlanId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Backup

AWS Backup define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
backup:ChangeableForDays	Filtra el acceso por el valor del ChangeableForDays parámetro	Numérico
backup:CopyTargetOrgPaths	Filtra el acceso por unidad organizativa.	ArrayOfString
backup:CopyTargets	Filtra el acceso por el ARN de una bóveda de respaldo	ArrayOfARN
backup:FrameworkArns	Filtra el acceso mediante el Framework ARNs	ArrayOfARN
backup:Index	Filtra el acceso por el valor del parámetro Index	Cadena
backup:MaxRetentionDays	Filtra el acceso por el valor del MaxRetentionDays parámetro	Numérico
backup:MinRetentionDays	Filtra el acceso por el valor del MinRetentionDays parámetro	Numérico
backup:MpaApprovalTeamArn	Filtra el acceso del equipo de aprobación de la MPA (ARN) a una bóveda de respaldo	ARN

Acciones, recursos y claves de condición para AWS Backup Gateway.

AWS Backup Gateway (prefijo de servicio:`backup-gateway`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Backup Gateway
- Tipos de recursos definidos por AWS Backup Gateway
- Claves de condición para AWS Backup Gateway

Acciones definidas por AWS Backup Gateway

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateGatewayToServer	Otorga permiso a Associate GatewayToServer	Escritura	gateway*		
			hypervisor*		
Backup	Concede permiso a Backup.	Escritura	virtualmachine*		
CreateGateway	Otorga permiso a CreateGateway	Escritura		aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
DeleteGateway	Otorga permiso a DeleteGateway	Escritura	gateway*		
DeleteHypervisor	Otorga permiso a DeleteHypervisor	Escritura	hypervisor*		
DisassociateGatewayFromServer	Otorga permiso a DisassociateGatewayFromServer	Escritura	gateway*		
GetBandwidthRateLimitSchedule	Otorga permiso a GetBandwidthRateLimitSchedule	Lectura	gateway*		
GetGateway	Otorga permiso a GetGateway	Lectura	gateway*		
GetHypervisor	Otorga permiso a GetHypervisor	Lectura	hypervisor*		
GetHypervisorPropertyMappings	Otorga permiso a GetHypervisorPropertyMappings	Lectura	hypervisor*		
GetVirtualMachine	Otorga permiso a GetVirtualMachine	Lectura	virtualmachine*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportHypervisorConfiguration	Otorga permiso a ImportHypervisorConfiguration	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	Otorga permiso a ListGateways	Lectura			
ListHypervisors	Otorga permiso a ListHypervisors	Lectura			
ListTagsForResource	Otorga permiso a ListTagsForResource	Lectura	gateway		
			hypervisor		
			virtualmachine		
ListVirtualMachines	Otorga permiso a ListVirtualMachines	Lectura			
PutBandwidthRateLimitSchedule	Otorga permiso a PutBandwidthRateLimitSchedule	Escritura	gateway*		
PutHypervisorPropertyMappings	Otorga permiso a PutHypervisorPropertyMappings	Escritura	hypervisor*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutMaintenanceStartTime	Otorga permiso a PutMaintenanceStartTime	Escritura	gateway*		
Restore	Concede permiso a Restore.	Escritura	hypervisor*		
StartVirtualMachinesMetadataSync	Otorga permiso a StartVirtualMachinesMetadataSync	Escritura	hypervisor*		iam:PassRole
TagResource	Otorga permiso a TagResource	Etiquetado	gateway		
			hypervisor		
			virtualmachine		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestHypervisorConfiguration	Otorga permiso a TestHypervisorConfiguration	Escritura	gateway*		
UntagResource	Otorga permiso a UntagResource	Etiquetado	gateway		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	Otorga permiso a UpdateGatewayInformation	Escritura	gateway*		
UpdateGatewaySoftwareNow	Otorga permiso a UpdateGatewaySoftwareNow	Escritura	gateway*		
UpdateHypervisor	Otorga permiso a UpdateHypervisor	Escritura	gateway*		

Tipos de recursos definidos por AWS Backup Gateway

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
gateway	`arn:${Partition}:backup-gateway:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
hypervisor	`arn:${Partition}:backup-gateway:${Region}:${Account}:hypervisor/${HypervisorId}`	aws:ResourceTag/${TagKey}
virtualmachine	`arn:${Partition}:backup-gateway:${Region}:${Account}:vm/${VirtualmachineId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Backup Gateway

AWS Backup Gateway define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de AWS Backup Search

AWS Backup Search (prefijo de servicio:`backup-search`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Backup Search
- Tipos de recursos definidos por AWS Backup Search
- Claves de condición para AWS Backup Search

Acciones definidas por AWS Backup Search

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSearchJob	Otorga permiso para obtener los detalles de un puesto de búsqueda	Lectura	searchJob*		
GetSearchResultExportJob	Otorga permiso para obtener detalles de un trabajo de exportación de resultados de búsqueda	Lectura	searchExportJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSearchJobBackups	Otorga permiso para incluir las copias de seguridad en el ámbito de un trabajo de búsqueda	Lectura	searchJob*		
ListSearchJobResults	Otorga permiso para enumerar los resultados de un trabajo de búsqueda	Lectura	searchJob*		
ListSearchJobs	Otorga permiso para incluir en una lista los trabajos de búsqueda	Enumeración			
ListSearchResultExportJobs	Otorga permiso para enumerar los trabajos de exportación de los resultados de búsqueda	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	searchExportJob		
			searchJob		
StartSearchJob	Otorga permiso para crear un trabajo de búsqueda	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartSearchResultExportJob	Otorga permiso para iniciar un trabajo de exportación para un trabajo de búsqueda existente	Escritura	searchJob*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopSearchJob	Otorga permiso para detener un trabajo de búsqueda en curso	Escritura	searchJob*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	searchExportJob		
			searchJob		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	searchExportJob		
			searchJob		
				aws:TagKeys	

Tipos de recursos definidos por AWS Backup Search

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
searchJob	`arn:${Partition}:backup-search:${Region}:${Account}:search-job/${ResourceId}`	aws:ResourceTag/${TagKey}
searchExportJob	`arn:${Partition}:backup-search:${Region}:${Account}:search-export-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Backup Search

AWS Backup Search define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el almacenamiento de AWS Backup

AWS Backup Storage (prefijo de servicio:`backup-storage`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el almacenamiento de AWS Backup
- Tipos de recursos definidos por el almacenamiento de AWS Backup
- Claves de condición para el almacenamiento de AWS Backup

Acciones definidas por el almacenamiento de AWS Backup

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CommitBackupJob [solo permiso]	Otorga permiso para confirmar el trabajo de copia de seguridad	Escritura			
DeleteObjects [solo permiso]	Otorga permiso para eliminar objetos	Escritura			
DescribeBackupJob [solo permiso]	Otorga permiso para describir un trabajo de copia de seguridad	Escritura			
GetBaseBackup [solo permiso]	Otorga permiso para obtener una copia de seguridad base	Escritura			
GetChunk [solo permiso]	Otorga permiso para obtener datos de un punto de recuperación para un trabajo de restauración	Escritura			
GetIncrementalBaseBackup [solo permiso]	Otorga permiso para obtener una copia de seguridad incremental base	Escritura			
GetObjectMetadata [solo permiso]	Otorga permiso para obtener metadatos de un punto de recuperación para un trabajo de restauración	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListChunks [solo permiso]	Otorga permiso para enumerar los datos desde un punto de recuperación para un trabajo de restauración	Escritura			
ListObjects [solo permiso]	Otorga permiso para enumerar los datos desde un punto de recuperación para un trabajo de restauración	Escritura			
MountCapsule [solo permiso]	Asocia una clave de KMS a un almacén de copia de seguridad.	Escritura			
NotifyObjectComplete [solo permiso]	Otorga permiso para marcar un dato cargado como completado para un trabajo de copia de seguridad	Escritura			
PutChunk [solo permiso]	Concede permiso para cargar datos en un punto de recuperación AWS gestionado por Backup para un trabajo de backup	Escritura			
PutObject [solo permiso]	Otorga permiso para poner un objeto	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartObject [solo permiso]	Concede permiso para cargar datos en un punto de recuperación AWS gestionado por Backup para un trabajo de backup	Escritura			
UpdateObjectComplete [solo permiso]	Otorga permiso para actualizar el objeto completo	Escritura			

Tipos de recursos definidos por el almacenamiento de AWS Backup

AWS El almacenamiento de backup no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al almacenamiento de AWS Backup, especifique `"Resource": "*"` en su política.

Claves de condición para el almacenamiento de AWS Backup

Backup Storage no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Batch

AWS Batch (prefijo de servicio:`batch`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Batch
- Tipos de recursos definidos por AWS Batch
- Claves de condición para AWS Batch

Acciones definidas por AWS Batch

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelJob	Otorga permiso para cancelar un trabajo en una cola de trabajos de AWS Batch en su cuenta	Escritura	job*		
CreateComputeEnvironment	Otorga permiso para crear un entorno de procesamiento AWS por lotes en su cuenta	Escritura	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	Otorga permiso para crear un recurso consumible de AWS Batch en tu cuenta	Escritura	consumable-resource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	Otorga permiso para crear una cola de trabajos de AWS Batch en su cuenta	Escritura	compute-environment*		
			job-queue*	aws:RequestTag/${TagKey} aws:TagKeys	
			scheduling-policy		
CreateSchedulingPolicy	Otorga permiso para crear una política de programación de AWS Batch en su cuenta	Escritura	scheduling-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteComputeEnvironment	Otorga permiso para eliminar un entorno de procesamiento AWS por lotes en su cuenta	Escritura	compute-environment*		
DeleteConsumableResource	Otorga permiso para eliminar un recurso consumible de AWS Batch de tu cuenta	Escritura	consumable-resource*		
DeleteJobQueue	Otorga permiso para eliminar una cola de trabajos de AWS Batch en su cuenta	Escritura	job-queue*		
DeleteSchedulingPolicy	Otorga permiso para eliminar una política de programación de AWS Batch en su cuenta	Escritura	scheduling-policy*		
DeregisterJobDefinition	Otorga permiso para anular el registro de una definición de trabajo AWS por lotes en su cuenta	Escritura	job-definition-revision*		
DescribeComputeEnvironments	Otorga permiso para describir uno o más entornos de procesamiento AWS por lotes en su cuenta	Lectura			
DescribeConsumableResource	Otorga permiso para describir uno o más recursos consumibles de AWS Batch en su cuenta	Lectura	consumable-resource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeJobDefinitions	Otorga permiso para describir una o más definiciones de tareas de AWS Batch en su cuenta	Lectura			
DescribeJobQueues	Otorga permiso para describir una o más colas de trabajos de AWS Batch en su cuenta	Lectura			
DescribeJobs	Otorga permiso para describir una lista de trabajos de AWS Batch en su cuenta	Lectura			
DescribeSchedulingPolicies	Otorga permiso para describir una o más políticas de programación de AWS Batch en su cuenta	Lectura			
GetJobQueueSnapshot	Otorga permiso para obtener una instantánea de una cola de trabajos de AWS Batch en su cuenta	Lectura	job-queue*		
ListConsumableResources	Otorga permiso para incluir los recursos consumibles de AWS Batch en su cuenta	Enumeración			
ListJobs	Otorga permiso para enumerar trabajos para una cola de trabajos AWS por lotes específica en su cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListJobsByConsumableResource	Otorga permiso para enumerar los trabajos AWS por lotes que requieren un recurso consumible específico en su cuenta	Enumeración	consumable-resource*		
ListSchedulingPolicies	Otorga permiso para incluir las políticas de programación de AWS Batch en su cuenta	Lectura			
ListTagsForResource	Otorga permiso para incluir etiquetas para un recurso de AWS Batch en su cuenta	Lectura	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
RegisterJobDefinition	Otorga permiso para registrar una definición de trabajo AWS por lotes en su cuenta	Escritura	job-definition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			consumable-resource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				batch:EKSRunAsUser batch:EKSRunAsGroup batch:EKSPrivileged batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SubmitJob	Otorga permiso para enviar un trabajo de AWS Batch desde una definición de trabajo de su cuenta	Escritura	job*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
			job-definition*		
			job-queue*		
			consumable-resource		
TagResource	Otorga permiso para etiquetar un recurso de AWS Batch en tu cuenta	Etiquetado	compute-environment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	Otorga permiso para finalizar un trabajo en una cola de trabajos de AWS Batch de su cuenta	Escritura	job*		
UntagResource	Otorga permiso para desetiquetar un recurso de AWS Batch de tu cuenta	Etiquetado	compute-environment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
				aws:TagKeys	
UpdateComputeEnvironment	Otorga permiso para actualizar un entorno de procesamiento AWS por lotes en su cuenta	Escritura	compute-environment*		
UpdateConsumableResource	Otorga permiso para actualizar un recurso consumible de AWS Batch en tu cuenta	Escritura	consumable-resource*		
UpdateJobQueue	Otorga permiso para actualizar una cola de trabajos de AWS Batch en su cuenta	Escritura	job-queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			compute-environment		
			scheduling-policy		
UpdateSchedulingPolicy	Otorga permiso para actualizar una política de programación de AWS Batch en su cuenta	Escritura	scheduling-policy*		

Tipos de recursos definidos por AWS Batch

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
compute-environment	`arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}`	aws:ResourceTag/${TagKey}
job-queue	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
job-definition	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}`	
job-definition-revision	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:batch:${Region}:${Account}:job/${JobId}`	aws:ResourceTag/${TagKey}
scheduling-policy	`arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}`	aws:ResourceTag/${TagKey}
consumable-resource	`arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Batch

AWS Batch define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
batch:AWSLogsCreateGroup	Filtra el acceso según el controlador de registro especificado para determinar si se creará el grupo de awslogs para los registros.	Bool
batch:AWSLogsGroup	Filtra el acceso según el grupo de awslogs donde se encuentran los registros.	Cadena
batch:AWSLogsRegion	Filtra el acceso según la región a la que se envían los registros.	Cadena
batch:AWSLogsStreamPrefix	Filtra el acceso según el prefijo de flujo de registro awslogs.	Cadena
batch:EKSImage	Filtra el acceso según la imagen que se usa para iniciar un contenedor para un trabajo de Amazon EKS	Cadena
batch:EKSNamespace	Filtra el acceso por el espacio de nombres de un clúster utilizado para ejecutar el pod para un trabajo de Amazon EKS	Cadena
batch:EKSPrivileged	Filtra el acceso según el valor de parámetro privilegiado y especificado que determina si al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similar al usuario raíz, para un trabajo de Amazon EKS	Bool

Claves de condición	Descripción	Tipo
batch:EKS RunAsGroup	Filtra el acceso por el ID numérico de grupo (gid) especificado que se usa para iniciar un contenedor en un trabajo de Amazon EKS	Numérico
batch:EKS RunAsUser	Filtra el acceso por el ID numérico de usuario (uid) especificado que se usa para iniciar un contenedor en un trabajo de Amazon EKS	Numérico
batch:EKS ServiceAccountName	Filtra el acceso por el nombre de la cuenta de servicio usada para ejecutar el pod para un trabajo de Amazon EKS	Cadena
batch:Image	Filtra el acceso según la imagen que se usa para iniciar un contenedor	Cadena
batch:LogDriver	Filtra el acceso según el controlador de registro que se usa para el contenedor.	Cadena
batch:Privileged	Filtra el acceso según el valor de parámetro privilegiado y específico que determina si al contenedor se le conceden privilegios elevados en la instancia de contenedor de host, similares a los de un usuario raíz.	Bool
batch:ShareIdentifier	Filtra el acceso según el shareIdentifier que se usa dentro del trabajo de envío.	Cadena
batch:User	Filtra el acceso según el nombre de usuario o UID numérico que se usa dentro del contenedor.	Cadena

Acciones, recursos y claves de condición para Amazon Bedrock

Amazon Bedrock (prefijo de servicio: `bedrock`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de IAM permisos.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Bedrock
- Tipos de recursos definidos por Amazon Bedrock
- Claves de condición para Amazon Bedrock

Acciones definidas por Amazon Bedrock

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de

recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Concede permiso para configurar la entrega de registros suministrados por un proveedor para una base de conocimientos	Administración de permisos	knowledge-base		
ApplyGuardrail	Concede permiso para aplicar una barrera de protección	Lectura	guardrail*		
			guardrail-profile		
AssociateAgentCollaborator	Otorga permiso para asociar a otro agente existente como	Escritura	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	colaborador a un agente existente				
AssociateAgentKnowledgeBase	Concede permiso para asociar una base de conocimiento a un agente	Escritura	agent*		
			knowledge-base*		
AssociateThirdPartyKnowledgeBase [solo permiso]	Concede permiso para usar una plataforma de terceros para almacenar datos de conocimiento	Escritura		bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	
BatchDeleteEvaluationJob	Concede permiso para eliminar por lotes la lista de trabajos de evaluación de Bedrock	Escritura	evaluation-job*		
CallWithBearerToken	Otorga permiso para usar el token de portador	Lectura			
CreateAgent	Concede permiso para crear un nuevo agente y un alias de agente de prueba que apunte a la versión del agente DRAFT	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentActionGroup	Concede permiso para crear un nuevo grupo de acciones en un agente existente	Escritura	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentAlias	Concede permiso para crear un nuevo alias para un agente	Escritura	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprint	Otorga permiso para crear un modelo de salida personalizado a partir de la automatización de datos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprintVersion	Otorga permiso para crear una nueva versión de un plano existente	Escritura	blueprint*		
CreateCustomModel	Otorga permiso para crear un modelo personalizado en Bedrock	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataAutomationProject	Otorga permiso para crear un proyecto de automatización de datos	Escritura	blueprint		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Concede permiso para crear un origen de datos	Escritura	knowledge-base*		
CreateEvaluationJob	Concede permiso para crear un trabajo para modelos de base de evaluación o modelos personalizados	Escritura	custom-model*		
			default-prompt-router*		
			foundation-model*		
			prompt-router*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFlow	Concede permiso para crear un flujo de peticiones	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowAlias	Concede permiso para crear un alias de un flujo de peticiones	Escritura	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowVersion	Concede permiso para crear una versión inmutable de un flujo de peticiones	Escritura	flow*		
CreateFoundationModelAgreement	Concede permiso para crear un nuevo acuerdo de modelo de base	Escritura			
CreateGuardrail	Concede permiso para crear una nueva barrera de protección	Escritura	guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGuardrailVersion	Concede permiso para crear una nueva versión de barrera de protección	Escritura	guardrail*		
CreateInferenceProfile	Otorga permiso para crear perfiles de inferencia	Escritura	application-inference-profile*		
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvocation	Otorga permiso para crear una nueva invocación en una sesión existente	Escritura	session*		
CreateKnowledgeBase	Concede permiso para crear una base de conocimientos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMarketplaceModelEndpoint	Otorga permiso para crear un punto final modelo de mercado	Escritura			
CreateModelCopyJob	Concede permiso para crear un trabajo para copiar un modelo personalizado entre regiones o entre cuentas	Escritura	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCustomizationJob	Concede permiso para crear un trabajo para personalizar el modelo con sus datos de entrenamiento personalizados	Escritura	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelEvaluationJob	Concede permiso para crear un trabajo para modelos de base de evaluación o modelos personalizados	Escritura	custom-model*		
			foundation-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelImportJob	Concede permiso para crear un trabajo para importar el modelo a Bedrock	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelInvocationJob	Concede permiso para crear un trabajo de invocación de modelo nuevo	Escritura	custom-model*		
			foundation-model*		
			model-invocation-job*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePrompt	Concede permiso para crear una petición	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptRouter	Otorga permiso para crear un router rápido personalizado		application-inference-profile*		
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptVersion	Concede permiso para crear una versión de una petición		prompt*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProvisionedModelThroughput	Concede permiso para crear un nuevo rendimiento de modelo aprovisionado	Escritura	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSession	Otorga permiso para crear una sesión nueva	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Concede permiso para eliminar un agente que haya creado anteriormente	Escritura	agent*		
DeleteAgentActionGroup	Concede permiso para eliminar un actionGroup que haya creado anteriormente	Escritura	agent*		
DeleteAgentAlias	Otorga permiso para eliminar una AgentAlias que haya creado anteriormente	Escritura	agent-alias*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAgentMemory	Concede permiso para eliminar la memoria existente de un alias	Escritura	agent-alias*		
DeleteAgentVersion	Concede permiso para eliminar una versión de agente que haya creado anteriormente	Escritura	agent*		
DeleteBlueprint	Otorga permiso para eliminar un plan de automatización de datos	Escritura	blueprint*		
DeleteCustomModel	Concede permiso para eliminar un modelo personalizado que haya creado anteriormente	Escritura	custom-model*		
DeleteDataAutomationProject	Otorga permiso para eliminar un proyecto de automatización de datos	Escritura	data-automation-project*		
DeleteDataSource	Concede permiso para eliminar un origen de datos	Escritura	knowledge-base*		
DeleteFlow	Concede permiso para eliminar un flujo de peticiones	Escritura	flow*		
DeleteFlowAlias	Concede permiso para eliminar un alias de un flujo de peticiones	Escritura	flow-alias*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFlowVersion	Concede permiso para eliminar una versión de un flujo de peticiones	Escritura	flow*		
DeleteFoundationModelAgreement	Concede permiso para eliminar un acuerdo de modelo de base que haya creado anteriormente	Escritura			
DeleteGuardrail	Concede permiso para eliminar una barrera de protección o su versión	Escritura	guardrail*		
DeleteImportedModel	Concede permiso para eliminar el modelo de Bedrock importado previamente creado	Escritura	imported-model*		
DeleteInferenceProfile	Otorga permiso para eliminar perfiles de inferencia	Escritura	application-inference-profile*		
DeleteKnowledgeBase	Concede permiso para eliminar una base de conocimientos	Escritura	knowledge-base*		
DeleteKnowledgeBaseDocuments	Otorga permiso para eliminar documentos de una base de conocimientos	Escritura	knowledge-base*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMarketplaceModelAgreement	Otorga permiso para cancelar la suscripción a un modelo de mercado básico basado en AWS el mercado	Escritura			
DeleteMarketplaceModelEndpoint	Otorga permiso para eliminar un punto final modelo de mercado	Escritura	bedrock-marketplace-model-endpoint*		
DeleteModelInvocationLoggingConfiguration	Concede permiso para eliminar una configuración de registro de invocación existente	Escritura			
DeletePrompt	Concede permiso para eliminar una petición o su versión	Escritura	prompt* prompt-version*		
DeletePromptRouter	Otorga permiso para eliminar un router de mensajes personalizado	Escritura	prompt-router*		
DeleteProvisionedModelThroughput	Concede permiso para eliminar un rendimiento de modelo aprovisionado que haya creado anteriormente	Escritura	provisioned-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcePolicy [solo permiso]	Elimina una política de recursos de Bedrock creada previamente	Escritura	custom-model*		
DeleteSession	Otorga permiso para eliminar una sesión que haya creado anteriormente	Escritura	session*		
DeregisterMarketplaceModelEndpoint	Otorga permiso para anular el registro de un punto final modelo Marketplace para que no se pueda utilizar en Bedrock Marketplace	Escritura	bedrock-marketplace-model-endpoint*		
DetectGeneratedContent	Concede permiso para detectar si el contenido proporcionado se genera mediante Amazon Bedrock	Lectura	foundation-model*		
DisassociateAgentCollaborator	Otorga permiso para desasociar a un colaborador al que hayas asociado anteriormente	Escritura	agent*		
DisassociateAgentKnowledgeBase	Concede permiso para desasociar una base de conocimiento de agente	Escritura	agent*		
			knowledge-base*		
EndSession	Otorga permiso para finalizar una sesión que haya creado anteriormente	Escritura	session*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateQuery	Otorga permiso para generar consultas asociadas a las entradas del usuario	Lectura			
GetAgent	Concede permiso para recuperar un agente existente	Lectura	agent*		
GetAgentActionGroup	Concede permiso para recuperar un grupo de acciones existente	Lectura	agent*		
GetAgentAlias	Concede permiso para recuperar un alias existente	Lectura	agent-alias*		
GetAgentCollaborator	Otorga permiso para recuperar un colaborador existente	Lectura	agent*		
GetAgentKnowledgeBase	Concede permiso para describir una base de conocimiento asociada a un agente	Lectura	agent* knowledge-base*		
GetAgentMemory	Concede permiso para recuperar memoria existente para un alias	Lectura	agent-alias*		
GetAgentVersion	Concede permiso para recuperar una versión de agente existente	Lectura	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAsyncInvoke	Otorga permiso para obtener las propiedades asociadas a una invocación asíncrona que haya enviado	Lectura	async-invoke*		
GetBlueprint	Otorga permiso para recuperar un plan existente para la automatización de datos	Lectura	blueprint*		
GetBlueprintRecommendation [solo permiso]	Otorga permiso para recuperar la recomendación del plan	Lectura			
GetCustomModel	Concede permiso para obtener las propiedades asociadas a un modelo personalizado de Bedrock que haya creado	Lectura	custom-model*		
GetDataAutomationProject	Otorga permiso para recuperar un proyecto de automatización de datos existente	Lectura	data-automation-project*		
GetDataAutomationStatus	Otorga permiso para recuperar el estado de un trabajo de invocación de automatización de datos	Lectura	data-automation-invocation-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDataSource	Concede permiso para recuperar un origen de datos existente	Lectura	knowledge-base*		
GetEvaluationJob	Concede permiso para obtener las propiedades asociadas a un trabajo de evaluación. Utilizar esta operación para obtener el estado de un trabajo de evaluación	Lectura	evaluation-job*		
GetExecutionFlowSnapshot	Otorga permiso para recuperar la definición de flujo para una ejecución de flujo	Lectura	flow*		
			flow-alias*		
			flow-execution*		
GetFlow	Concede permiso para recuperar un flujo de peticiones existente	Lectura	flow*		
GetFlowAlias	Concede permiso para recuperar un alias existente de un flujo de peticiones	Lectura	flow-alias*		
GetFlowExecution	Otorga permiso para recuperar una ejecución existente de un alias de flujo	Lectura	flow*		
			flow-alias*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			flow-execution*		
GetFlowVersion	Concede permiso para recuperar una versión existente de un flujo de peticiones	Lectura	flow*		
GetFoundationModel	Concede permiso para obtener las propiedades asociadas a un modelo de base de Bedrock	Lectura	foundation-model*		
GetFoundationModelAvailability	Concede permiso para obtener la disponibilidad de un modelo de base	Lectura			
GetGuardrail	Concede permiso para recuperar una barrera de protección o su versión	Lectura	guardrail*		
GetImportedModel	Concede permiso para obtener las propiedades asociadas al modelo de Bedrock importado	Lectura	imported-model*		
GetInferenceProfile	Concede permiso para obtener las propiedades asociadas a un perfil de inferencia	Lectura	application-inference-profile*		
			inference-profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIngestionJob	Concede permiso para recuperar un trabajo de incorporación existente	Lectura	knowledge-base*		
GetInvocationStep	Otorga permiso para obtener un paso de invocación de una sesión	Lectura	session*		
GetKnowledgeBase	Concede permiso para recuperar una base de conocimiento existente	Lectura	knowledge-base*		
GetKnowledgeBaseDocuments	Otorga permiso para obtener detalles de los documentos de una base de conocimientos	Lectura	knowledge-base*		
GetMarketplaceModelEndpoint	Otorga permiso para obtener las propiedades de un punto final modelo de mercado	Lectura	bedrock-marketplace-model-endpoint*		
GetModelCopyJob	Concede permiso para obtener las propiedades asociadas a un trabajo de copia de modelo. Utilizar esta operación para obtener el estado de un trabajo de copia de modelo	Lectura	model-copy-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetModelCustomizationJob	Concede permiso para obtener las propiedades asociadas con un trabajo de personalización de modelos. Utilice esta operación para obtener el estado de un trabajo de personalización de modelos	Lectura	model-customization-job*		
GetModelEvaluationJob	Concede permiso para obtener las propiedades asociadas con un trabajo de evaluación de modelos. Utilice esta operación para obtener el estado de un trabajo de evaluación de modelos	Lectura	model-evaluation-job*		
GetModelImportJob	Concede permiso para obtener las propiedades asociadas a un trabajo de importación de modelos y se utiliza para obtener el estado de un trabajo de importación de modelos	Lectura	model-import-job*		
GetModelInvocationJob	Concede permiso para recuperar un trabajo de invocación de modelo	Lectura	model-invocation-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetModelInvocationLoggingConfiguration	Concede permiso para recuperar una configuración de registro de invocación existente	Lectura			
GetPrompt	Concede permiso para recuperar una petición existente o su versión	Lectura	prompt*		
			prompt-version*		
GetPromptRouter	Otorga permiso para obtener las propiedades asociadas a un router rápido	Lectura	default-prompt-router*		
			prompt-router*		
GetProvisionedModelThroughput	Concede permiso para recuperar un rendimiento de modelo aprovisionado	Lectura	provisioned-model*		
GetResourcePolicy [solo permiso]	Obtiene el documento de política de recursos de un recurso de Bedrock	Lectura	custom-model*		
GetSession	Otorga permiso para recuperar una sesión existente	Lectura	session*		
GetUseCaseForModelAccess	Concede permiso para recuperar un caso de uso para acceder a modelos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
IngestKnowledgeBaseDocuments	Otorga permiso para incorporar documentos directamente a una base de conocimientos	Escritura	knowledge-base*		
InvokeAgent	Concede permiso para enviar la entrada del usuario (solo texto) al alias de un agente de Bedrock	Lectura	agent-alias*		
InvokeBlueprintRecommendationAsync [solo permiso]	Otorga permiso para invocar recomendaciones de planos de forma asíncrona	Escritura	data-automation-profile*		
InvokeBuilder [solo permiso]	Concede permiso para utilizar el generador conversacional, que ayuda a crear recursos de Bedrock compatibles	Escritura			
InvokeDataAutomationAsync	Otorga permiso para invocar un trabajo de automatización de datos de Bedrock	Escritura	blueprint*		
			data-automation-profile*		
			data-automation-project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeFlow	Concede permiso para invocar un flujo de peticiones con la entrada del usuario	Lectura	flow-alias*		
InvokeInlineAgent	Otorga permiso para enviar las entradas del usuario (solo texto) al agente en línea de Bedrock	Lectura		bedrock:InlineAgentName	
InvokeModel	Concede permiso para invocar el modelo de Bedrock especificado para ejecutar la inferencia utilizando la entrada proporcionada en el cuerpo de la solicitud	Lectura	application-inference-profile*		
			async-invoke*		
			bedrock-marketplace-model-endpoint*		
			default-prompt-router*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		
				bedrock:InferenceProfileArn bedrock:PromptRouterArn aws:RequestTag/${TagKey} aws:TagKeys bedrock:GuardrailIdentifier	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InvokeModelWithResponseStream	Concede permiso para invocar el modelo Bedrock especificado para ejecutar la inferencia utilizando la entrada proporcionada en el cuerpo de la solicitud con respuesta de transmisión	Lectura	application-inference-profile*		
			bedrock-marketplace-model-endpoint*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				bedrock:InferenceProfileArn bedrock:PromptRouterArn bedrock:GuardrailIdentifier	
ListAgentActionGroups	Concede permiso para enumerar grupos de acciones en un agente	Enumeración	agent*		
ListAgentAliases	Concede permiso para enumerar alias de un agente	Enumeración	agent*		
ListAgentCollaborators	Otorga permiso para incluir a un agente en la lista de colaboradores	Enumeración	agent*		
ListAgentKnowledgeBases	Concede permiso para enumerar las bases de conocimiento asociadas a un agente	Enumeración	agent*		
ListAgentVersions	Concede permiso para enumerar versiones de agente existentes	Enumeración	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAgents	Concede permiso para enumerar los agentes existentes	Enumeración			
ListAsyncInvokes	Otorga permiso para obtener una lista de las invocaciones asíncronas que ha enviado	Enumeración			
ListBlueprints	Otorga permiso para enumerar los planos existentes para la automatización de datos	Enumeración	data-automation-project		
ListCustomModels	Concede permiso para obtener una lista de modelos personalizados de Bedrock que ha creado	Enumeración			
ListDataAutomationProjects	Otorga permiso para enumerar los proyectos de automatización de datos existentes	Enumeración	blueprint		
ListDataSources	Concede permiso para enumerar los orígenes de datos existentes en una base de conocimiento	Enumeración	knowledge-base*		
ListEvaluationJobs	Concede permiso para obtener la lista de trabajos de evaluación que ha enviado	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFlowAliases	Concede permiso para enumerar los alias existentes de un flujo de peticiones	Enumeración	flow*		
ListFlowExecutionEvents	Otorga permiso para recuperar eventos para la ejecución de un flujo	Enumeración	flow*		
			flow-alias*		
			flow-execution*		
ListFlowExecutions	Otorga permiso para enumerar las ejecuciones de un flujo o un alias de flujo	Enumeración	flow*		
			flow-alias		
ListFlowVersions	Concede permiso para enumerar las versiones existentes de un flujo de peticiones	Enumeración	flow*		
ListFlows	Concede permiso para enumerar flujos de peticiones existentes	Enumeración			
ListFoundationModelAgreementOffers	Concede permiso para obtener una lista de ofertas de acuerdo de modelo de base	Enumeración			
ListFoundationModels	Concede permiso para enumerar los modelos de base de Bedrock que puede utilizar	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGuardrails	Concede permiso para enumerar barreras de protección o sus versiones	Enumeración	guardrail		
ListImportedModels	Concede permiso para obtener la lista de modelos de Bedrock importados	Enumeración			
ListInferenceProfiles	Concede permiso para enumerar los perfiles de inferencia que puede utilizar	Enumeración			
ListIngestionJobs	Concede permiso para enumerar trabajos de incorporación en un origen de datos	Enumeración	knowledge-base*		
ListInvocationSteps	Otorga permiso para obtener la lista de los pasos de invocación de una sesión	Enumeración	session*		
ListInvocations	Otorga permiso para enumerar las invocaciones de una sesión	Enumeración	session*		
ListKnowledgeBaseDocuments	Otorga permiso para incluir documentos en una base de conocimientos	Enumeración	knowledge-base*		
ListKnowledgeBases	Concede permiso para enumerar las bases de conocimiento existentes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMarketplaceModelEndpoints	Otorga permiso para enumerar los puntos finales del modelo de mercado que puede utilizar	Lectura			
ListModelCopyJobs	Concede permiso para obtener la lista de trabajos de copia de modelos que ha enviado	Enumeración			
ListModelCustomizationJobs	Concede permiso para obtener la lista de trabajos de personalización de modelos que ha enviado	Enumeración			
ListModelEvaluationJobs	Concede permiso para obtener la lista de trabajos de evaluación de modelos que ha enviado	Enumeración			
ListModelImportJobs	Concede permiso para obtener la lista de trabajos de importación de modelos	Enumeración			
ListModelInvocationJobs	Concede permiso para enumerar trabajos de invocación de modelo que haya creado anteriormente	Enumeración			
ListPromptRouters	Otorga permiso para enumerar los enrutadores rápidos que puede usar	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPrompts	Concede permiso para enumerar peticiones existentes	Enumeración	prompt		
ListProvisionedModelThroughputs	Concede permiso para enumerar los rendimientos de modelo aprovisionado que haya creado anteriormente	Enumeración			
ListSessions	Otorga permiso para enumerar las sesiones existentes	Enumeración			
ListTagsForResource	Concede permiso para listar etiquetas para un recurso de Bedrock	Lectura	agent*		
			agent-alias*		
			application-inference-profile*		
			async-invoke*		
			blueprint*		
			custom-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			data-automation-invocation-job*		
			data-automation-project*		
			evaluation-job*		
			flow*		
			flow-alias*		
			guardrail*		
			imported-model*		
			knowledge-base*		
			model-copy-job*		
			model-customization-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			model-evaluation-job*		
			model-import-job*		
			model-invocation-job*		
			prompt*		
			prompt-router*		
			prompt-version*		
			provisioned-model*		
			session*		
OptimizePrompt	Otorga permiso para optimizar un mensaje con las entradas del usuario	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PrepareAgent	Concede permiso para preparar un agente existente para recibir solicitudes de tiempo de ejecución	Escritura	agent*		
PrepareFlow	Concede permiso para aplicar los cambios más recientes realizados en un flujo de peticiones, de modo que se reflejen en tiempo de ejecución	Escritura	flow*		
PutFoundationModelEntitlement	Concede permiso para dar el derecho de acceso a un modelo de base	Escritura			
PutInvocationStep	Otorga permiso para incluir un paso de invocación en una invocación en sesión	Escritura	session*		
PutModelInvocationLoggingConfiguration	Concede permiso para crear una configuración de registro de invocación	Escritura			
PutResourcePolicy [solo permiso]	Agrega una política de recursos para un recurso de Bedrock	Escritura	custom-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
PutUseCaseForModelAccess	Concede permiso para poner un caso de uso para el acceso de modelo	Escritura			
RegisterMarketplaceModelEndpoint	Otorga permiso para registrar un punto final de SageMaker como punto final modelo de mercado	Escritura	bedrock-marketplace-model-endpoint*		
RenderPrompt [solo permiso]	Otorga permiso para renderizar una solicitud existente o su versión	Lectura	prompt* prompt-version*		
Rerank	Otorga permiso para clasificar los documentos en función de las entradas del usuario	Escritura			
Retrieve	Concede permiso para recuperar datos incorporados de una base de conocimiento	Lectura	knowledge-base*		
RetrieveAndGenerate	Concede permiso para enviar la entrada del usuario para realizar la recuperación y la generación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartFlowExecution	Otorga permiso para iniciar la ejecución de un alias de flujo	Escritura	flow*		
			flow-alias*		
StartIngestionJob	Concede permiso para iniciar un trabajo de incorporación	Escritura	knowledge-base*		
StopEvaluationJob	Concede permiso para detener un trabajo de evaluación en curso	Escritura	evaluation-job*		
StopFlowExecution	Otorga permiso para detener la ejecución de un alias de flujo	Escritura	flow*		
			flow-alias*		
			flow-execution*		
StopIngestionJob	Concede permiso para detener un trabajo de ingesta	Escritura	knowledge-base*		
StopModelCustomizationJob	Concede permiso para detener un trabajo de personalización del modelo Bedrock mientras está en progreso	Escritura	model-customization-job*		
StopModelInvocationJob	Concede permiso para detener un trabajo de invocación de modelo que haya iniciado anteriormente	Escritura	model-invocation-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar un recurso Bedrock	Etiquetado	agent		
			agent-alias		
			application-inference-profile		
			async-invoke		
			blueprint		
			custom-model		
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para quitar la etiqueta de un recurso Bedrock	Etiquetado	agent		
			agent-alias		
			application-inference-profile		
			async-invoke		
			blueprint		
			custom-model		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys	
UpdateAgent	Concede permiso para actualizar un agente existente	Escritura	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAgentActionGroup	Concede permiso para actualizar un grupo de acciones existente	Escritura	agent*		
UpdateAgentAlias	Concede permiso para actualizar un alias existente	Escritura	agent-alias*		
UpdateAgentCollaborator	Otorga permiso para actualizar a un colaborador existente	Escritura	agent*		
UpdateAgentKnowledgeBase	Concede permiso para actualizar una base de conocimiento asociada a un agente	Escritura	agent*		
			knowledge-base*		
UpdateBlueprint	Otorga permiso para actualizar un plan de automatización de datos	Escritura	blueprint*		
UpdateDataAutomationProject	Otorga permiso para actualizar un proyecto de automatización de datos	Escritura	data-automation-project*		
			blueprint		
UpdateDataSource	Concede permiso para actualizar un origen de datos	Escritura	knowledge-base*		
UpdateFlow	Concede permiso para actualizar un flujo de peticiones	Escritura	flow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFlowAlias	Concede permiso para actualizar la configuración de un alias de un flujo de peticiones	Escritura	flow-alias*		
UpdateGuardrail	Concede permiso para actualizar una barrera de protección	Escritura	guardrail*		
			guardrail-profile		
UpdateKnowledgeBase	Concede permiso para actualizar una base de conocimientos	Escritura	knowledge-base*		
UpdateMarketplaceModelEndpoint	Otorga permiso para actualizar el punto final de un modelo de mercado	Escritura	bedrock-marketplace-model-endpoint*		
UpdatePrompt	Concede permiso para actualizar una petición	Escritura	prompt*		
UpdateProvisionedModelThroughput	Concede permiso para actualizar un rendimiento de modelo aprovisionado que haya creado anteriormente	Escritura	custom-model*		
			foundation-model*		
			provisioned-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSession	Otorga permiso para actualizar una sesión existente	Escritura	session*		
ValidateFlowDefinition	Otorga permiso para validar las definiciones de flujo rápido	Lectura			

Tipos de recursos definidos por Amazon Bedrock

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
foundation-model	`arn:${Partition}:bedrock:${Region}::foundation-model/${ResourceId}`	
async-invoke	`arn:${Partition}:bedrock:${Region}:${Account}:async-invoke/${ResourceId}`	aws:ResourceTag/${TagKey}
inference-profile	`arn:${Partition}:bedrock:${Region}:${Account}:inference-profile/${ResourceId}`	
default-prompt-router	`arn:${Partition}:bedrock:${Region}:${Account}:default-prompt-router/${ResourceId}`	

Tipos de recurso	ARN	Claves de condición
prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:prompt-router/${ResourceId}	
application-inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:application-inference-profile/${ResourceId}	aws:ResourceTag/${TagKey}
custom-model	arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}	aws:ResourceTag/${TagKey}
provisioned-model	arn:${Partition}:bedrock:${Region}:${Account}:provisioned-model/${ResourceId}	aws:ResourceTag/${TagKey}
model-customization-job	arn:${Partition}:bedrock:${Region}:${Account}:model-customization-job/${ResourceId}	aws:ResourceTag/${TagKey}
agent	arn:${Partition}:bedrock:${Region}:${Account}:agent/${AgentId}	aws:ResourceTag/${TagKey}
agent-alias	arn:${Partition}:bedrock:${Region}:${Account}:agent-alias/${AgentId}/${AgentAliasId}	aws:ResourceTag/${TagKey}
knowledge-base	arn:${Partition}:bedrock:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
model-evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
model-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-invocation-job/${JobIdentifier}	aws:ResourceTag/${TagKey}
guardrail	arn:${Partition}:bedrock:${Region}:${Account}:guardrail/${GuardrailId}	aws:ResourceTag/${TagKey}
guardrail-profile	arn:${Partition}:bedrock:${Region}:${Account}:guardrail-profile/${ResourceId}	
flow	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}	aws:ResourceTag/${TagKey}
flow-alias	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}	aws:ResourceTag/${TagKey}
flow-execution	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}/execution/${FlowExecutionId}	
model-copy-job	arn:${Partition}:bedrock:${Region}:${Account}:model-copy-job/${ResourceId}	aws:ResourceTag/${TagKey}
prompt	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
prompt-version	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}:${PromptVersion}	aws:ResourceTag/${TagKey}
model-import-job	arn:${Partition}:bedrock:${Region}:${Account}:model-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
imported-model	arn:${Partition}:bedrock:${Region}:${Account}:imported-model/${ResourceId}	aws:ResourceTag/${TagKey}
bedrock-marketplace-model-endpoint	arn:${Partition}:bedrock:${Region}:${Account}:marketplace/model-endpoint/all-access	
data-automation-project	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-project/${ProjectId}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:bedrock:${Region}:${Account}:blueprint/${BlueprintId}	aws:ResourceTag/${TagKey}
data-automation-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-invocation/${JobId}	aws:ResourceTag/${TagKey}
data-automation-profile	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-profile/${ProfileId}	
session	arn:${Partition}:bedrock:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Bedrock

Amazon Bedrock define las siguientes claves de condición que se pueden usar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso creando solicitudes basadas en el conjunto de valores permitidos para cada una de las etiquetas obligatorias	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso al tener acciones basadas en el valor de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra el acceso creando solicitudes basadas en la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
bedrock:GuardrailIdentifier	Filtra el acceso por lo GuardrailIdentifier que contiene GuardrailArn o lo siguiente GuardrailArn: NumericVersion	ARN
bedrock:InferenceProfileArn	Filtra el acceso según el perfil de inferencia especificado	ARN
bedrock:InlineAgentName	Filtra el acceso por los nombres de los agentes en línea, que se utilizarán en los nombres de las InvokeInlineAgent API	Cadena
bedrock:PromptRouterArn	Filtra el acceso mediante el router rápido especificado	ARN
bedrock:ThirdParty	Filtra el acceso mediante el secretArn que contiene las credenciales de la plataforma de terceros	ARN

Claves de condición	Descripción	Tipo
KnowledgeBaseCredentialsSecretArn		

Acciones, recursos y claves de condición para AWS Billing

AWS Billing (prefijo de servicio:`billing`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Billing
- Tipos de recursos definidos por AWS Billing
- Claves de condición de AWS Billing

Acciones definidas por AWS Billing

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBillingView	Otorga permiso para crear una vista de facturación	Escritura	billingview*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBillingView	Otorga permiso para eliminar una vista de facturación	Escritura	billingview*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [solo permiso]	Otorga permiso para eliminar una política de recursos de visualización de facturación	Administración de permisos	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData [solo permiso]	Concede permiso para realizar consultas sobre información de facturación	Lectura			
GetBillingDetails [solo permiso]	Concede permiso para ver información de facturación de elementos de línea detallada	Lectura			
GetBillingNotifications [solo permiso]	Otorga permiso para ver las notificaciones enviadas por AWS relacionadas con la información de facturación de su cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBillingPreferences [solo permiso]	Concede permiso para ver preferencias de facturación tales como instancia reservada, Savings Plans y uso compartido de créditos	Lectura			
GetBillingView	Otorga permiso para obtener los metadatos de una vista de facturación específica	Lectura	billingview*		
				aws:ResourceTag/${TagKey}	
GetContractInformation [solo permiso]	Concede permiso para ver la información contractual de la cuenta, incluyendo número del contrato, nombres de las organizaciones de los usuarios finales, números de orden de compra y si la cuenta se utiliza para prestar servicios a clientes del sector público	Lectura			
GetCredits [solo permiso]	Concede permiso para ver créditos que se han canjeado	Lectura			
GetIAMAccessPreference [solo permiso]	Concede permiso para recuperar el estado de la preferencia de facturación Allow IAM Access (Permitir acceso de IAM)	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourcePolicy	Otorga permiso para obtener la vista de facturación especificada en la política de recursos	Administración de permisos	billingview*		
				aws:ResourceTag/${TagKey}	
GetSellerOfRecord [solo permiso]	Concede permiso para recuperar el vendedor registrado predeterminado de la cuenta	Lectura			
ListBillingViews	Otorga permiso para obtener una lista de todas las vistas de facturación disponibles	Lectura			
ListSourceViewsForBillingView	Otorga permiso para obtener la lista de vistas de origen para una vista de facturación específica	Enumeración	billingview*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Otorga permiso para obtener la lista de etiquetas de una vista de facturación específica	Lectura	billingview*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutContractInformation [solo permiso]	Concede permiso para establecer la información contractual de la cuenta, los nombres de las organizaciones de los usuarios finales y si la cuenta se utiliza para prestar servicios a clientes del sector público	Escritura			
PutResourcePolicy [solo permiso]	Otorga permiso para poner una política de recursos de visualización de facturación	Administración de permisos	billingview*		
				aws:ResourceTag/${TagKey}	
RedeemCredits [solo permiso]	Otorga permiso para canjear cualquier crédito AWS	Escritura			
TagResource	Otorga permiso para añadir etiquetas a una vista de facturación específica	Etiquetado	billingview*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar una etiqueta de una vista de facturación específica	Etiquetado	billingview*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateBillingPreferences [solo permiso]	Concede permiso para actualizar preferencias de facturación tales como instancia reservada, Savings Plans y uso compartido de créditos	Escritura			
UpdateBillingView	Otorga permiso para actualizar una vista de facturación	Escritura	billingview*		
				aws:ResourceTag/${TagKey}	
UpdateIAMAccessPreference [solo permiso]	Concede permiso para actualizar la preferencia de facturación Allow IAM Access (Permitir acceso de IAM)	Escritura			

Tipos de recursos definidos por AWS Billing

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Billing

AWS Billing define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para exportaciones de datos de AWS Billing y gestión de costos

AWS Billing Además, Cost Management Data Exports (prefijo de servicio:`bcm-data-exports`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por exportaciones de datos de AWS Billing y gestión de costos
- Tipos de recursos definidos por exportaciones de datos de AWS Billing y gestión de costos
- Claves de condición para las exportaciones de datos de AWS Billing y gestión de costos

Acciones definidas por exportaciones de datos de AWS Billing y gestión de costos

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateExport	Concede permiso para crear una exportación	Escritura	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteExport	Otorga permiso para eliminar una exportación	Escritura	export*		
				aws:ResourceTag/${TagKey}	
GetExecution	Otorga permiso para obtener las ejecuciones de una exportación	Lectura	export*		
				aws:ResourceTag/${TagKey}	
GetExport	Otorga permiso para obtener una exportación	Lectura	export*		
				aws:ResourceTag/${TagKey}	
GetTable	Otorga permiso para obtener los detalles de una tabla	Lectura	table*		
ListExecutions	Otorga permiso para enumerar todas las ejecuciones de una exportación	Enumeración	export*		
				aws:ResourceTag/${TagKey}	
ListExports	Concede permiso para enumerar todas las exportaciones	Enumeración			
ListTables	Concede permiso para enumerar las tablas disponibles	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	export*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	export*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	export*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateExport	Concede permiso para actualizar una exportación	Escritura	export*		
			table*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por exportaciones de datos de AWS Billing y gestión de costos

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
export	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:export/${Identifier}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:table/${Identifier}`	

Claves de condición para las exportaciones de datos de AWS Billing y gestión de costos

AWS Billing Además, Cost Management Data Exports define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de acciones, recursos y condiciones de la calculadora de precios de AWS Billing And Cost Management

AWS Billing Además, la calculadora de precios de gestión de costes (prefijo de servicio:`bcm-pricing-calculator`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la calculadora de precios de AWS Billing And Cost Management
- Tipos de recursos definidos por la calculadora de precios de AWS Billing And Cost Management
- Claves de estado para la calculadora de precios de AWS Billing And Cost Management

Acciones definidas por la calculadora de precios de AWS Billing And Cost Management

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBillEstimate	Otorga permiso para crear una nueva estimación de la factura. Se incurre en un cargo si las estimaciones de facturas se realizan correctamente	Escritura	bill-scenario		
CreateBillScenario	Otorga permiso para crear un nuevo escenario de facturación	Escritura			
CreateBillScenarioCommitmentModification	Otorga permiso para crear nuevos compromisos o eliminar un compromiso existente de un escenario de proyecto de ley específico	Escritura	bill-scenario*		
CreateBillScenarioUsageModification	Otorga permiso para crear un uso en el escenario de facturación especificado	Escritura	bill-scenario*		
CreateWorkloadEstimate	Otorga permiso para crear una nueva estimación de la carga de trabajo	Escritura			
CreateWorkloadEstimateUsage	Otorga permiso para crear un uso en la estimación de carga de trabajo especificada	Escritura	workload-estimate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBillEstimate	Otorga permiso para eliminar la estimación de la factura	Escritura	bill-estimate*		
DeleteBillScenario	Otorga permiso para eliminar un escenario de facturación	Escritura	bill-scenario*		
DeleteBillScenarioCommitmentModification	Otorga permiso para eliminar los compromisos recién agregados del escenario de facturación especificado	Escritura	bill-scenario*		
DeleteBillScenarioUsageModification	Otorga permiso para eliminar el uso recién agregado del escenario de facturación especificado	Escritura	bill-scenario*		
DeleteWorkloadEstimate	Otorga permiso para eliminar la estimación de carga de trabajo especificada	Escritura	workload-estimate*		
DeleteWorkloadEstimateUsage	Otorga permiso para eliminar el uso recién agregado de la estimación de carga de trabajo especificada	Escritura	workload-estimate*		
GetBillEstimate	Otorga permiso para recuperar los detalles de una factura estimada, incluido el costo estimado	Lectura	bill-estimate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBillScenario	Otorga permiso para recuperar la información asociada a un escenario de facturación	Lectura	bill-scenario*		
GetPreferences	Otorga permiso para recuperar las preferencias de tipo de tarifa aplicables a la cuenta	Lectura			
GetWorkloadEstimate	Otorga permiso para recuperar la información asociada a una estimación de la carga de trabajo	Lectura	workload-estimate*		
ListBillEstimateCommitments	Otorga permiso para enumerar los compromisos asociados a la estimación de la factura especificada	Enumeración	bill-estimate*		
ListBillEstimateInputCommitmentModifications	Otorga permiso para enumerar los compromisos agregados o eliminados para una estimación de factura específica	Enumeración	bill-estimate*		
ListBillEstimateInputUsageModifications	Otorga permiso para incluir los usos añadidos o modificados para una estimación de factura específica	Enumeración	bill-estimate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBillEstimateLineItems	Otorga permiso para incluir las partidas de resultados de una estimación de factura específica	Enumeración	bill-estimate*		
ListBillEstimates	Otorga permiso para incluir las estimaciones de los proyectos de ley	Enumeración			
ListBillScenarioCommitmentModifications	Otorga permiso para enumerar los compromisos incluidos en un escenario de proyecto de ley	Enumeración	bill-scenario*		
ListBillScenarioUsageModifications	Otorga permiso para enumerar las líneas de uso de un escenario de facturación específico	Enumeración	bill-scenario*		
ListBillScenarios	Otorga permiso para enumerar escenarios de facturación	Enumeración			
ListTagsForResource	Concede permiso para devolver una lista de etiquetas de un recurso	Etiquetado			
ListWorkloadEstimateUsage	Otorga permiso para enumerar las líneas de uso para la estimación de carga de trabajo especificada	Enumeración	workload-estimate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorkloadEstimates	Otorga permiso para enumerar las estimaciones de carga de trabajo	Enumeración			
TagResource	Otorga permiso para agregar una etiqueta a un recurso.	Etiquetado		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado		aws:TagKeys	
UpdateBillEstimate	Otorga permiso para actualizar el nombre y la hora estimados de la factura	Escritura	bill-estimate*		
UpdateBillScenario	Otorga permiso para actualizar el nombre y la fecha y hora de caducidad del escenario de facturación especificado	Escritura	bill-scenario*		
UpdateBillScenarioCommitmentModification	Otorga permiso para actualizar el grupo de compromisos en el escenario de facturación especificado	Escritura	bill-scenario*		
UpdateBillScenarioUsageModification	Otorga permiso para actualizar la cantidad de uso, la hora de uso y el grupo de uso en el escenario de facturación especificado	Escritura	bill-scenario*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePreferences	Otorga permiso para actualizar las preferencias de tipo de tarifa de la cuenta	Escritura			
UpdateWorkloadEstimate	Otorga permiso para actualizar el nombre y la fecha y hora de caducidad de la estimación de carga de trabajo especificada	Escritura	workload-estimate*		
UpdateWorkloadEstimateUsage	Otorga permiso para actualizar la cantidad de uso y el grupo de uso en la estimación de carga de trabajo especificada en función del identificador de uso	Escritura	workload-estimate*		

Tipos de recursos definidos por la calculadora de precios de AWS Billing And Cost Management

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
bill-estimate	`arn:${Partition}:bcm-pricing-calculator:${Region}:${Account}:bill-estimate/${BillEstimateId}`	
bill-scenario	`arn:${Partition}:bcm-pricing-calculator:${Region}:${Account}:bill-scenario/${BillScenarioId}`	
workload-estimate	`arn:${Partition}:bcm-pricing-calculator:${Region}:${Account}:workload-estimate/${WorkloadEstimateId}`	

Claves de estado para la calculadora de precios de AWS Billing And Cost Management

AWS Billing Y la calculadora de precios de gestión de costes define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Billing Conductor

AWS Billing Conductor (prefijo de servicio:`billingconductor`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Billing Conductor
- Tipos de recursos definidos por AWS Billing Conductor
- Claves de condición de AWS Billing Conductor

Acciones definidas por AWS Billing Conductor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateAccounts	Concede permiso para asociar de una a 30 cuentas a un grupo de facturación	Escritura	billinggroup*		
AssociatePricingRules	Concede permiso para asociar reglas de precios	Escritura	pricingplan*		
			pricingrule*		
BatchAssociateResourcesToCustomLineItem	Concede permiso para asociar recursos por lotes a un porcentaje de partida personalizada	Escritura	customlineitem*		
BatchDisassociateResourcesFromCustomLineItem	Concede permiso para desasociar recursos por lotes a un porcentaje de partida personalizada	Escritura	customlineitem*		
CreateBillingGroup	Concede permiso para crear un grupo de facturación	Escritura	pricingplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomLineItem	Concede permiso para crear una partida personalizada	Escritura	billinggroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingPlan	Concede permiso para crear un plan de precios	Escritura	pricingrule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingRule	Concede permiso para crear una regla de precios	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBillingGroup	Concede permiso para eliminar un grupo de facturación	Escritura	billinggroup*		
DeleteCustomLineItem	Concede permiso para eliminar una partida personalizada	Escritura	customlineitem*		
DeletePricingPlan	Concede permiso para eliminar un plan de precios	Escritura	pricingplan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePricingRule	Concede permiso para eliminar una regla de precios	Escritura	pricingrule*		
DisassociateAccounts	Concede permiso para desvincular entre una y 30 cuentas de un grupo de facturación	Escritura	billinggroup*		
DisassociatePricingRules	Concede permiso para desasociar reglas de precios	Escritura	pricingplan*		
			pricingrule*		
GetBillingGroupCostReport	Concede permiso para visualizar el informe de costos del grupo de facturación especificado	Lectura	billinggroup*		
ListAccountAssociations	Concede permiso para enumerar las cuentas vinculadas de la cuenta del pagador para un período de facturación determinado, al tiempo que proporciona el grupo de facturación al que pertenecen las cuentas vinculadas	Enumeración			
ListBillingGroupCostReports	Concede permiso para visualizar el informe de costos del grupo de facturación	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBillingGroups	Concede permiso para visualizar los detalles de los grupos de facturación	Lectura			
ListCustomLineItemVersions	Otorga permiso para ver versiones de elementos de línea personalizados	Lectura	customlineitem*		
ListCustomLineItems	Concede permiso para visualizar los detalles de las partidas personalizadas	Lectura			
ListPricingPlans	Concede permiso para visualizar los detalles de los planes de precios	Lectura			
ListPricingPlansAssociatedWithPricingRule	Concede permiso para enumerar los planes de precios asociados a una regla de precios	Enumeración	pricingrule*		
ListPricingRules	Concede permiso para visualizar los detalles de las reglas de precios	Lectura			
ListPricingRulesAssociatedToPricingPlan	Concede permiso para enumerar las reglas de precios asociadas a un plan de precios	Enumeración	pricingplan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourcesAssociatedToCustomLineItem	Concede permiso para enumerar los recursos asociados a un porcentaje de partida personalizada	Enumeración	customlineitem*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso	Lectura	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	billinggroup		
			customlineitem		
			pricingplan		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys	
UpdateBillingGroup	Concede permiso para actualizar un grupo de facturación	Escritura	billinggroup*		
UpdateCustomLineItem	Concede permiso para actualizar una partida personalizada	Escritura	customlineitem*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePricingPlan	Concede permiso para actualizar un plan de precios	Escritura	pricingplan*		
UpdatePricingRule	Concede permiso para actualizar una regla de precios	Escritura	pricingrule*		

Tipos de recursos definidos por AWS Billing Conductor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
billinggroup	`arn:${Partition}:billingconductor::${Account}:billinggroup/${BillingGroupId}`	aws:ResourceTag/${TagKey}
pricingplan	`arn:${Partition}:billingconductor::${Account}:pricingplan/${PricingPlanId}`	aws:ResourceTag/${TagKey}
pricingrule	`arn:${Partition}:billingconductor::${Account}:pricingrule/${PricingRuleId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
customlineitem	`arn:${Partition}:billingconductor::${Account}:customlineitem/${CustomLineItemId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Billing Conductor

AWS Billing Conductor define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Billing Console

AWS Billing La consola (prefijo de servicio:`aws-portal`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la consola de AWS Billing
- Tipos de recursos definidos por la consola de AWS Billing
- Claves de condición de la consola de AWS Billing

Acciones definidas por la consola de AWS Billing

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConsoleActionSetEnforced [solo permiso]	Concede permiso para ver si se utilizan acciones de IAM existentes o detalladas para controlar la autorización en las consolas de facturación, administración de costos y cuenta	Lectura			
ModifyAccount [solo permiso]	Permitir o denegar permisos a los usuarios de IAM para modificar la Configuración de la cuenta	Escritura			
ModifyBilling [solo permiso]	Permitir o denegar permisos a los usuarios de IAM para	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	modificar la configuración de facturación				
ModifyPaymentMethods [solo permiso]	Permitir o denegar permisos a los usuarios de IAM para modificar los métodos de pago	Escritura			
UpdateConsoleActionSetEnforced [solo permiso]	Concede permiso para cambiar si se utilizarán acciones de IAM existentes o detalladas para controlar la autorización en las consolas de facturación, administración de costos y cuenta	Escritura			
ViewAccount [solo permiso]	Permitir o denegar permisos a los usuarios de IAM para ver la configuración de la cuenta	Lectura			
ViewBilling [solo permiso]	Permitir o denegar permisos a los usuarios de IAM para ver páginas de facturación en la consola	Lectura			
ViewPaymentMethods [solo permiso]	Permitir o denegar permisos a los usuarios de IAM para ver los métodos de pago	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ViewUsage [solo permiso]	Permita o deniegue a los usuarios de IAM el permiso para ver AWS los informes de uso	Lectura			

Tipos de recursos definidos por la consola de AWS Billing

AWS Billing La consola no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la consola de AWS Billing , especifique `"Resource": "*"` en su política.

Claves de condición de la consola de AWS Billing

La consola de facturación no tiene claves de contexto específicas de servicios que se puedan usar en el elemento `Condition` de declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Braket

Amazon Braket (prefijo de servicio: `braket`) proporciona los siguientes recursos, acciones y claves de condición específicos para servicios para usarlos en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Braket

- Tipos de recurso definidos por Amazon Braket
- Claves de condición de Amazon Braket

Acciones definidas por Amazon Braket

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptUserAgreement [solo permiso]	Concede permiso para aceptar el acuerdo de usuario de Amazon Braket	Escritura			
CancelJob	Concede permiso para cancelar un trabajo	Escritura	job*		
CancelQuantumTask	Otorga permiso para cancelar una tarea cuántica.	Escritura	quantum-task*		
CreateJob	Concede permiso para crear un trabajo.	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateQuantumTask	Otorga permiso para crear una tarea cuántica.	Escritura		aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetDevice	Otorga permiso para recuperar información sobre los dispositivos disponibles en Amazon Braket.	Lectura			
GetJob	Otorga permiso para recuperar trabajos.	Lectura	job*		
GetQuantumTask	Otorga permiso para recuperar tareas cuánticas.	Lectura	quantum-task*		
GetServiceLinkedRoleStatus [solo permiso]	Concede permiso para comprobar si se ha creado el rol vinculado al servicio Amazon Braket	Lectura			
GetUserAgreementStatus [solo permiso]	Concede permiso para comprobar si la cuenta ha aceptado el acuerdo de usuario de Amazon Braket	Lectura			
ListTagsForResource	Otorga permiso para enumerar las etiquetas que se han aplicado al recurso de tarea cuántica o al trabajo.	Lectura	job quantum-task		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchDevices	Otorga permiso para buscar dispositivos disponibles en Amazon Braket.	Lectura			
SearchJobs	Otorga permiso para buscar trabajos.	Lectura			
SearchQuantumTasks	Otorga permiso para buscar tareas cuánticas.	Lectura			
TagResource	Otorga permiso para agregar una o varias etiquetas a una tarea cuántica o un trabajo híbrido.	Etiquetado	job		
			quantum-task		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una o varias etiquetas de un recurso de tarea cuántica o de un trabajo. Las etiquetas se componen de un par clave-valor	Etiquetado	job		
			quantum-task		
				aws:TagKeys	

Tipos de recurso definidos por Amazon Braket

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
quantum-task	`arn:${Partition}:braket:${Region}:${Account}:quantum-task/${RandomId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:braket:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Braket

Amazon Braket define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Budget Service

AWS Budget Service (prefijo de servicio:`budgets`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Budget Service
- Tipos de recursos definidos por AWS Budget Service
- Claves de condición para AWS Budget Service

Acciones definidas por AWS Budget Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Las acciones de esta tabla no lo son APIs, sino que son permisos que otorgan acceso a los Administración de facturación y costos de AWS APIs presupuestos de acceso.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBudgetAction	Concede permiso para configurar una respuesta que se ejecutará una vez que su presupuesto supere	Escritura	budgetAction*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	un umbral de presupuesto específico. Para crear una acción presupuestaria con etiquetas también se requiere el permiso «presupuestos:TagResource»			aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	Otorga permiso para eliminar una acción asociada a un presupuesto específico	Escritura	budgetAction*		
DescribeBudgetAction	Otorga permiso para recuperar los detalles de una acción presupuestaria específica asociada a un presupuesto	Lectura	budgetAction*		
DescribeBudgetActionHistories	Otorga permiso para recuperar una vista histórica de los estados de las acciones presupuestarias asociados a una acción presupuestaria concreta. Estos estados son “Standby” (En espera), “Pending” (Pendiente) y “Executed” (Ejecutada)	Lectura	budgetAction*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBudgetActionsForAccount	Otorga permiso para recuperar los detalles de todas las acciones presupuestarias asociadas a su cuenta	Lectura			
DescribeBudgetActionsForBudget	Otorga permiso para recuperar los detalles de todas las acciones presupuestarias asociadas a un presupuesto	Lectura	budget*		
ExecuteBudgetAction	Otorga permiso para iniciar una acción presupuestaria pendiente, así como para revertir una acción presupuestaria ejecutada anteriormente	Escritura	budgetAction*		
ListTagsForResource	Concede permiso para ver etiquetas de recursos para un presupuesto o una acción de presupuesto	Lectura	budget		
			budgetAction		
ModifyBudget	Concede permiso para crear y modificar presupuestos, así como para editar los detalles del presupuesto. Para crear un presupuesto con etiquetas también se requiere el permiso «presupuestos:TagResource»	Escritura	budget*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para aplicar etiquetas de recursos a un presupuesto o acción de presupuesto. También se necesita para crear un presupuesto o una acción de presupuesto con etiquetas	Etiquetado	budget		
			budgetAction		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de recursos de un presupuesto o acción de presupuesto	Etiquetado	budget		
			budgetAction		
				aws:TagKeys	
UpdateBudgetAction	Otorga permiso para actualizar los detalles de una acción presupuestaria específica asociada a un presupuesto	Escritura	budgetAction*		iam:PassRole
ViewBudget	Otorga permiso para ver presupuestos y detalles del presupuesto	Lectura	budget*		

Tipos de recursos definidos por AWS Budget Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
budget	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
budgetAction	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}/action/${ActionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Claves de condición para AWS Budget Service

AWS Budget Service define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS BugBust

AWS BugBust (prefijo de servicio:`bugbust`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS BugBust
- Tipos de recursos definidos por AWS BugBust
- Claves de condición de AWS BugBust

Acciones definidas por AWS BugBust

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEvent [solo permiso]	Otorga permiso para crear un evento BugBust	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
EvaluateProfilingGroups [solo permiso]	Concede permiso para evaluar los grupos de perfiles registrados.	Write	Event*		
				aws:ResourceTag/${TagKey}	
GetEvent [solo permiso]	Concede permiso para ver detalles del cliente con respecto a un evento.	Read	Event*		
				aws:ResourceTag/${TagKey}	
GetJoinEventStatus [solo permiso]	Otorga permiso para ver el estado del intento de un BugBust jugador de unirse a un BugBust evento	Lectura	Event*		
				aws:ResourceTag/${TagKey}	
JoinEvent [solo permiso]	Concede permiso para unirse a un evento.	Write	Event*		
				aws:ResourceTag/${TagKey}	
ListBugs [solo permiso]	Concede permiso para ver los errores que se importaron en un evento para que los	Read	Event*		codeguru-reviewer:DescribeC

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	participantes trabajen sobre ellos.				odeReview codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	
ListEventParticipants [solo permiso]	Concede permiso para ver a los participantes de un evento.	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEventScores [solo permiso]	Concede permiso para ver las puntuaciones de los participantes dentro de un evento.	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEvents [solo permiso]	Otorga permiso para publicar BugBust eventos	Enumeración		aws:ResourceTag/${TagKey}	
ListProfilingGroups [solo permiso]	Concede permiso para ver los grupos de perfiles que se importaron en un evento para que los participantes trabajen sobre ellos.	Read	Event*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPullRequests [solo permiso]	Concede permiso para ver las solicitudes de extracción utilizadas por los participantes para enviar correcciones con respecto a los errores reclamados en un evento.	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [solo permiso]	Concede permiso para enumerar etiquetas para un recurso de Bugbust	Read	Event*		
				aws:ResourceTag/${TagKey}	
TagResource [solo permiso]	Concede permiso para etiquetar un recurso de Bugbust	Etiquetado	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [solo permiso]	Concede permiso para eliminar etiquetas de un recurso de Bugbust	Etiquetado	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEvent [solo permiso]	Otorga permiso para actualizar un BugBust evento	Escritura	Event*		codeguru-profiler: DescribeProfilingGroup codeguru-profiler: ListProfilingGroups codeguru-reviewer: DescribeCodeReview codeguru-reviewer: ListCodeReviews codeguru-reviewer: ListRecommendations codeguru-reviewer: TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					codeguru-reviewer:UnTagResource
				aws:ResourceTag/${TagKey}	
UpdateWorkItem [solo permiso]	Concede permiso para actualizar un elemento de trabajo como reclamado o no reclamado (error o grupo de perfiles).	Write	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	
UpdateWorkItemAdmin [solo permiso]	Concede permiso para actualizar el elemento de trabajo de un evento (error o grupo de perfiles).	Escritura	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS BugBust

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Event	`arn:${Partition}:bugbust:${Region}:${Account}:events/${EventId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS BugBust

AWS BugBust define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Certificate Manager

AWS Certificate Manager (prefijo de servicio:`acm`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Certificate Manager
- Tipos de recursos definidos por AWS Certificate Manager
- Claves de condición para AWS Certificate Manager

Acciones definidas por AWS Certificate Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTagsToCertificate	Otorga permiso para agregar una o más etiquetas a un certificado.	Etiquetado	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCertificate	Otorga permiso para eliminar un certificado y su clave privada asociada.	Write	certificate*		
DescribeCertificate	Otorga permiso para recuperar un certificado y sus metadatos.	Lectura	certificate*		
ExportCertificate	Otorga permiso para exportar un certificado exportable para su uso en cualquier lugar	Lectura	certificate*		
				acm:DomainNames	
GetAccountConfiguration	Otorga permiso para recuperar la configuración a nivel de cuenta de AWS Certificate Manager	Lectura			
GetCertificate	Otorga permiso para recuperar un certificado y una cadena de certificados para un ARN de certificados	Lectura	certificate*		
ImportCertificate	Otorga permiso para importar un certificado de terceros a AWS Certificate Manager (ACM)	Escritura	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCertificates	Otorga permiso para recuperar una lista del certificado ARNs y el nombre de dominio de cada ARN	Enumeración			
ListTagsForCertificate	Otorga permiso para enumerar las etiquetas que se han asociado a un certificado.	Lectura	certificate*		
PutAccountConfiguration	Otorga permiso para actualizar la configuración a nivel de cuenta en AWS Certificate Manager	Escritura			
RemoveTagsFromCertificate	Otorga permiso para eliminar una o más etiquetas de un certificado.	Etiquetado	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenewCertificate	Otorga permiso para renovar un certificado privado apto.	Write	certificate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RequestCertificate	Otorga permiso para solicitar un certificado público o privado.	Write		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLoggingPreference acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthorityArn acm:Export	
ResendValidationEmail	Otorga permiso para reenviar un correo electrónico a fin de solicitar la validación de propiedad de dominio.	Escritura	certificate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RevokeCertificate	Otorga permiso para revocar un certificado exportable	Escritura	certificate*		
				acm:DomainNames	
UpdateCertificateOptions	Concede el permiso para actualizar la configuración de un certificado. Se utiliza para especificar si desea activar o desactivar el registro de transparencia de certificados.	Escritura	certificate*		

Tipos de recursos definidos por AWS Certificate Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Certificate Manager

AWS Certificate Manager define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
acm:CertificateAuthority	Filtra el acceso por certificateAuthority en la solicitud. Se puede utilizar para restringir desde qué entidades de certificación se pueden emitir los certificados	Cadena
acm:CertificateTransparencyLogging	Filtra el acceso por certificateTransparencyLogging opción de la solicitud. Se establece en “HABILITADO” de forma predeterminada si no hay ninguna clave en la solicitud	Cadena
acm:DomainNames	Filtra el acceso por domainNames en la solicitud. Esta clave se puede utilizar para restringir qué dominios pueden incluirse en las solicitudes de certificados	ArrayOfString
acm:Export	Filtra el acceso por la opción de exportación de la solicitud. Se puede usar para restringir la creación de certificados que se pueden exportar	Cadena
acm:KeyAlgorithm	Filtra el acceso por keyAlgorithm en la solicitud	Cadena
acm:ValidationMethod	Filtra el acceso por validationMethod en la solicitud. Se establece en “CORREO ELECTRÓNICO” de forma predeterminada si no hay ninguna clave en la solicitud	Cadena
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Chatbot

AWS El Chatbot (prefijo de servicio:`chatbot`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Chatbot
- Tipos de recursos definidos por AWS Chatbot
- Claves de condición para AWS Chatbot

Acciones definidas por AWS Chatbot

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateToConfiguration	Otorga permiso para asociar un recurso a una configuración	Escritura	ChatbotConfiguration*		
			custom-action*		
CreateChimeWebhookConfiguration	Otorga permiso para crear una configuración de AWS Chatbot Chime Webhook	Escritura			
CreateCustomAction	Otorga permiso para crear una acción personalizada	Escritura			
CreateMicrosoftTeamsChannelConfiguration	Otorga permiso para crear una configuración de canal de AWS Chatbot Microsoft Teams	Escritura			
CreateSlackChannelConfiguration	Otorga permiso para crear una configuración de AWS canal de Chatbot en Slack	Escritura			
DeleteChimeWebhookConfiguration	Otorga permiso para eliminar una configuración de AWS Chatbot Chime Webhook	Escritura	ChatbotConfiguration*		
DeleteCustomAction	Otorga permiso para eliminar una acción personalizada	Escritura	custom-action*		
DeleteMicrosoftTea	Otorga permiso para eliminar una configuración de canal	Escritura	ChatbotConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
msChannelConfiguration	de AWS Chatbot Microsoft Teams				
DeleteMicrosoftTeamsConfiguredTeam	Otorga permiso para eliminar los Microsoft Teams configurados con AWS Chatbot en un Cuenta de AWS	Escritura			
DeleteMicrosoftTeamsUserIdentity	Otorga permiso para eliminar la identidad de AWS usuario de Microsoft Teams de un Chatbot	Escritura			
DeleteSlackChannelConfiguration	Otorga permiso para eliminar la configuración del canal de Slack de un AWS Chatbot	Escritura	ChatbotConfiguration*		
DeleteSlackUserIdentity	Otorga permiso para eliminar la identidad de un AWS usuario de Chatbot Slack	Escritura			
DeleteSlackWorkspaceAuthorization	Otorga permiso para eliminar la autorización del espacio de trabajo de Slack con AWS Chatbot, asociada a un Cuenta de AWS	Escritura			
DescribeChimeWebhookConfigurations	Otorga permiso para incluir todas las AWS configuraciones de Chatbot Chime Webhook en una cuenta AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSlackChannelConfigurations	Otorga permiso para enumerar todas las AWS configuraciones del canal de Slack del Chatbot en un Cuenta de AWS	Lectura			
DescribeSlackChannels	Otorga permiso para incluir todos los canales públicos de Slack en el espacio de trabajo de Slack conectados a la AWS cuenta integrada con el servicio de Chatbot AWS	Lectura			
DescribeSlackUserIdentities	Otorga permiso para describir las identidades de los usuarios de AWS Chatbot Slack	Lectura			
DescribeSlackWorkspaces	Otorga permiso para enumerar todos los espacios de trabajo de Slack autorizados conectados a la AWS cuenta integrada con el servicio de Chatbot AWS	Lectura			
DisassociateFromConfiguration	Otorga permiso para desasociar un recurso de una configuración	Escritura	ChatbotConfiguration* custom-action*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountPreferences	Otorga permiso para recuperar las preferencias de la cuenta de AWS Chatbot	Lectura			
GetCustomAction	Otorga permiso para realizar una acción personalizada	Lectura	custom-action*		
GetMicrosoftTeamsChannelConfiguration	Otorga permiso para obtener las configuraciones de canal de AWS Microsoft Teams de un solo Chatbot en un Cuenta de AWS	Lectura			
GetMicrosoftTeamsOauthParameters	Otorga permiso para generar OAuth parámetros para solicitar que el servicio de AWS Chatbot utilice el OAuth código de Microsoft Teams	Lectura			
GetSlackOauthParameters	Otorga permiso para generar OAuth parámetros para solicitar que el servicio de AWS Chatbot utilice el OAuth código de Slack	Lectura			
ListAssociations	Otorga permiso para enumerar los recursos asociados a una configuración	Lectura	ChatbotConfiguration*		
ListCustomActions	Otorga permiso para enumerar acciones personalizadas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMicrosoftTeamsChannelConfigurations	Otorga permiso para enumerar todas las configuraciones de canal de AWS Chatbot Microsoft Teams en un Cuenta de AWS	Lectura			
ListMicrosoftTeamsConfiguredTeams	Otorga permiso para enumerar todos los equipos de Microsoft conectados a la AWS cuenta incorporada con el servicio de Chatbot AWS	Lectura			
ListMicrosoftTeamsUserIdentities	Otorga permiso para describir las identidades de usuario de AWS Chatbot Microsoft Teams	Lectura			
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas asociadas a la configuración del AWS canal de Chatbot	Lectura			
RedeemMicrosoftTeamsOauthCode	Otorga permiso para canjear parámetros generados previamente con Microsoft APIs y adquirir OAuth tokens para ser utilizados por el servicio de AWS Chatbot	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RedeemSlackOauthCode	Otorga permiso para canjear parámetros generados previamente con la API de Slack, a fin de adquirir OAuth tokens para que los utilice el servicio de Chatbot AWS	Escritura			
TagResource	Otorga permiso para crear etiquetas en la configuración del AWS canal de Chatbot	Etiquetado			
UntagResource	Otorga permiso para eliminar etiquetas en la configuración del AWS canal de Chatbot	Etiquetado			
UpdateAccountPreferences	Otorga permiso para actualizar las preferencias de la cuenta de AWS Chatbot	Escritura			
UpdateChimeWebhookConfiguration	Otorga permiso para actualizar la configuración de un AWS Chatbot Chime Webhook	Escritura	ChatbotConfiguration*		
UpdateCustomAction	Otorga permiso para actualizar una acción personalizada	Escritura	custom-action*		
UpdateMicrosoftTeamsChannelConfiguration	Otorga permiso para actualizar la configuración del canal de AWS Microsoft Teams de un Chatbot	Escritura	ChatbotConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSlackChannelConfiguration	Otorga permiso para actualizar la configuración del canal de Slack de un AWS Chatbot	Escritura	ChatbotConfiguration*		

Tipos de recursos definidos por AWS Chatbot

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ChatbotConfiguration	`arn:${Partition}:chatbot::${Account}:chat-configuration/${ConfigurationType}/${ChatbotConfigurationName}`	
custom-action	`arn:${Partition}:chatbot::${Account}:custom-action/${ActionName}`	

Claves de condición para AWS Chatbot

Chatbot no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Chime

Amazon Chime (prefijo de servicio: `chime`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Chime
- Tipos de recursos definidos por Amazon Chime
- Claves de condición de Amazon Chime

Acciones definidas por Amazon Chime

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptDelegate	Otorga permiso para aceptar la invitación del delegado a compartir la administración de una cuenta de Amazon Chime con otra cuenta AWS	Escritura			
ActivateUsers	Otorga permiso para activar a los usuarios de una cuenta de Amazon Chime Enterprise.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddDomain	Otorga permiso para agregar un dominio a su cuenta de Amazon Chime.	Write			
AddOrUpdateGroups	Otorga permiso para agregar nuevos grupos de usuarios de Active Directory u Okta asociados a una cuenta de Amazon Chime Enterprise o actualizarlos.	Escritura			
AssociateChannelFlow	Otorga el permiso para asociar un flujo a un canal	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		
AssociatePhoneNumberWithUser	Otorga permiso para asociar un número de teléfono a un usuario de Amazon Chime.	Write			
AssociatePhoneNumbersWithVoiceConnector	Otorga permiso para asociar varios números de teléfono con Amazon Chime Voice Connector.	Write	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociatePhoneNumbersWithVoiceConnectorGroup	Otorga permiso para asociar varios números de teléfono con un grupo de Amazon Chime Voice Connector.	Escritura			
AssociateSigninDelegateGroupsWithAccount	Otorga permiso para asociar los grupos de delegados de inicio de sesión especificados a la cuenta de Amazon Chime especificada	Escritura			
AssociateVoiceConnectorConnect [solo permiso]	Otorga permiso para asociar la instancia de Amazon Connect especificada a un conector de voz de Amazon Chime	Escritura			
AuthorizeDirectory	Otorga permiso para autorizar un servicio de Active Directory para su cuenta de Amazon Chime Enterprise.	Write			
BatchCreateAttendee	Otorga permisos para crear nuevos asistentes para una reunión activa de Amazon Chime SDK	Escritura	meeting*		
BatchCreateChannelMembership	Concede permiso para agregar varios usuarios y bots a un canal	Escritura	app-instance-bot* app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channel*		
BatchCreateRoomMembership	Otorga permisos para agregar miembros de sala por lotes	Write			
BatchDeletePhoneNumber	Otorga permiso para mover hasta 50 números de teléfono a la cola de eliminación.	Write			
BatchSuspendUser	Otorga permiso para suspender hasta a 50 usuarios de una cuenta de Amazon Chime Team o Enterpris eLWA.	Write			
BatchUnsuspendUser	Otorga permiso para eliminar la suspensión de hasta 50 usuarios previamente suspendidos de la cuenta de Amazon Chime Enterpris eLWA especificada.	Escritura			
BatchUpdateAttendeeCapabilitiesExcept	Otorga permiso para actualizar AttendeeCapabilities , excepto las capacidades que se muestran en una tabla ExcludedAttendeeIds	Escritura	meeting*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchUpdatePhoneNumber	Otorga permiso para actualizar los detalles de los números de teléfono dentro del UpdatePhoneNumberRequestItem objeto para un máximo de 50 números de teléfono	Escritura			
BatchUpdateUser	Otorga permiso para actualizar los detalles de usuario dentro del UpdateUserRequestItem objeto para un máximo de 20 usuarios de la cuenta de Amazon Chime especificada	Escritura			
ChannelFlowCallback	Otorga el permiso para devolver la llamada de un mensaje en un canal	Escritura	channel*		
Connect	Otorga permiso para establecer una conexión de socket web para el usuario de instancia de la aplicación al punto de enlace de la sesión de mensajería	Write	app-instance-user*		
ConnectDirectory	Otorga permiso para conectar un servicio de Active Directory a su cuenta de Amazon Chime Enterprise.	Escritura			ds:ConnectDirectory

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccount	Otorga permiso para crear una cuenta de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura			
CreateApiKey	Otorga permiso para crear una nueva clave de acceso SCIM para su cuenta de Amazon Chime y configuración de Okta.	Escritura			
CreateAppInstance	Otorga permiso para crear una instancia de aplicación en el sistema Cuenta de AWS (los controles de acceso basados en etiquetas solo son compatibles con Identity-Chime). <region>.amazonaws.com (puntos de enlace)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceAdmin	Otorga permiso para ascender a un usuario o bot a AppInstanceAdmin	Escritura	app-instance*		
			app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAppInstanceBot	Otorga permiso para crear un bot dentro de un servidor AppInstance (los controles de acceso basados en etiquetas solo son compatibles con identity-chime). <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceUser	Otorga permiso para crear un usuario dentro de un AppInstance (los controles de acceso basados en etiquetas solo se admiten en Identity-Chime). <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAttendee	Otorga permisos para crear un nuevo asistente para una reunión activa de Amazon Chime SDK	Write	meeting*		
CreateBot	Otorga permiso para crear un bot para una cuenta de Amazon Chime Enterprise.	Escritura			
CreateCDRBucket	Otorga permiso para crear un nuevo bucket de S3 de registro de detalles de llamadas.	Escritura			s3:CreateBucket s3:ListAllMyBuckets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateChannel	Otorga permiso para crear un canal para una instancia de aplicación en Cuenta de AWS (los controles de acceso basados en etiquetas solo son compatibles con messaging-chime). <region>.amazonaws.com (puntos de enlace)	Escritura	app-instance-bot*		
			app-instance-user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelBan	Concede permiso para prohibir a un usuario o bot en un canal	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateChannelFlow	Otorga permiso para crear un flujo de canal para una instancia de aplicación en Cuenta de AWS (los controles de acceso basados en etiquetas solo son compatibles con messaging-chime). <region>.amazonaws.com (puntos de enlace)	Escritura	app-instance*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelMembership	Concede permiso para agregar a un usuario o bot a un canal	Escritura	app-instance-bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			app-instance-user*		
			channel*		
CreateChannelModerator	Otorga permiso para crear un moderador de canal	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateConnectAnalyticsConnector [solo permiso]	Otorga permiso para crear un conector de análisis de Amazon Connect en el Cuenta de AWS (los controles de acceso basados en etiquetas solo se admiten en timbres de voz). <region>.amazonaws.com (puntos de enlace)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateConnectCallTransferConnector [solo permiso]	Concede permiso para crear un conector de transferencia de llamadas de Amazon Connect en el Cuenta de AWS (los controles de acceso basados en etiquetas solo se admiten en timbres de voz). <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMediaCapturePipeline	Otorga permiso para crear un canal de captura de contenido multimedia (solo se admiten controles de acceso basados en etiquetas). media-pipelines-chime <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaConcatenationPipeline	Otorga permiso para crear un canal de concatenación de contenido multimedia (solo se admiten controles de acceso basados en etiquetas). media-pipelines-chime <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaInsightsPipeline	Otorga permiso para crear un canal de información sobre los medios (solo se admiten controles de acceso basados en etiquetas). media-pipelines-chime <region>.amazonaws.com (puntos finales)	Escritura	media-insights-pipeline-configuration*		chime:TagResource kinesisvideo:DescribeStream
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMediaInsightsPipelineConfiguration	Otorga permiso para crear una configuración de flujo de información multimedia (solo se admiten controles de acceso basados en etiquetas). media-pipelines-chime <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource iam:PassRole kinesis:DescribeStream s3:ListBucket
CreateMediaLiveConnectorPipeline	Otorga permiso para crear una canalización de conectores de media live (solo se admiten controles de acceso basados en etiquetas). media-pipelines-chime <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMediaPipelineKinesisVideoStreamPool	Otorga permiso para crear un pool de transmisiones de vídeo de Kinesis (solo se admiten controles de acceso basados en etiquetas en. media-pipelines-chime <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	kinesis:DescribeStream kinesisvideo:CreateStream kinesisvideo:GetDataEndpoint kinesisvideo:ListStreams
CreateMediaStreamPipeline	Otorga permiso para crear un canal de transmisión multimedia (solo se admiten controles de acceso basados en etiquetas en. media-pipelines-chime <region>. amazonaws.com (puntos finales)	Escritura	media-pipeline-kinesis-video-stream-pool*		kinesisvideo:DescribeStream kinesisvideo:GetDataEndpoint kinesisvideo:PutMedia

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMeeting	Concede permiso para crear una nueva reunión en la región de contenido multimedia especificada, sin asistentes iniciales (los controles de acceso basados en etiquetas solo se admiten en puntos de conexión meetings-chime.<region>.amazonaws.com)	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMeetingDialOut	Otorga permiso para llamar a un número de teléfono para unirse a la reunión específica de Amazon Chime SDK	Escritura	meeting*		
CreateMeetingWithAttendees	Concede permiso para crear una nueva reunión en la región de contenido multimedia especificada, con un conjunto de asistentes (los controles de acceso basados en etiquetas solo se admiten en puntos de conexión meetings-chime.<region>.amazonaws.com)	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePhoneNumberOrder	Otorga permiso para crear un pedido de números de teléfono con los operadores.	Write			
CreateProxySession	Otorga permiso para crear una sesión proxy para un Amazon Chime Voice Connector especificado	Write	voice-connector*		
CreateRoom	Otorga permisos para crear una sala	Write			
CreateRoomMembership	Otorga permisos para agregar un miembro a la sala	Escritura			
CreateSipMediaApplication	Otorga permiso para crear una aplicación multimedia SIP de Amazon Chime en Cuenta de AWS (los controles de acceso basados en etiquetas solo se admiten en campanillas de voz). <region>.amazonaws.com (puntos de enlace)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSipMediaApplicationCall	Otorga permiso para crear llamadas salientes para la aplicación multimedia SIP Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	sip-media-application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSipRule	Otorga permiso para crear una regla SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	sip-media-application		
CreateUser	Otorga permiso para crear un usuario en la cuenta de Amazon Chime especificada	Escritura			
CreateVoiceConnector	Otorga permiso para crear un conector de voz en el sistema Cuenta de AWS (los controles de acceso basados en etiquetas solo son compatibles con las campanillas de voz). <region>.amazonaws.com (puntos finales)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateConnectAnalyticsConnector chime:CreateConnectCallTransferConnector
CreateVoiceConnectorGroup	Otorga permiso para crear un grupo de conectores de voz de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	voice-connector		
CreateVoiceProfile	Concede permiso para crear un perfil de voz	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVoiceProfileDomain	Concede permiso para crear un dominio de perfil de voz (los controles de acceso basados en etiquetas solo se admiten en los puntos de conexión voice-chime.<region>.amazonaws.com)	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource kms:CreateGrant kms:DescribeKey
DeleteAccount	Otorga permiso para eliminar la cuenta de Amazon Chime especificada.	Escritura			
DeleteAccountOpenIdConfig	Otorga permiso para eliminar los OpenIdConfig atributos de su cuenta de Amazon Chime	Escritura			
DeleteApiKey	Otorga permiso para eliminar la clave de acceso SCIM especificada asociada a su cuenta de Amazon Chime y configuración de Okta.	Escritura			
DeleteAppInstance	Otorga permiso para eliminar un AppInstance	Escritura	app-instance*		
DeleteAppInstanceAdmin	Otorga permiso para degradar AppInstanceAdmin a un usuario o bot	Escritura	app-instance*		
			app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAppInstanceBot	Otorga permiso para eliminar un AppInstanceBot	Escritura	app-instance-bot*		
DeleteAppInstanceStreamingConfigurations	Otorga permiso para desactivar el streaming de datos de la instancia de aplicaciones	Escritura	app-instance*		
DeleteAppInstanceUser	Otorga permiso para eliminar un AppInstanceUser	Escritura	app-instance-user*		
DeleteAttendee	Otorga permisos para eliminar al asistente especificado de una reunión de Amazon Chime SDK	Write	meeting*		
DeleteCDRBucket	Otorga permiso para eliminar un bucket de S3 de registro de detalles de llamadas de su cuenta de Amazon Chime.	Write			s3:DeleteBucket
DeleteChannel	Da permiso para eliminar un canal.	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelBan	Concede permiso para eliminar a un usuario o bot de la lista de prohibición de un canal	Escritura	app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channel*		
DeleteChannelFlow	Otorga el permiso para eliminar un flujo de canal.	Escritura	channel*		
DeleteChannelMembership	Otorga permiso para eliminar a un miembro de un canal	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelMessage	Otorga permiso para eliminar un mensaje de canal	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelModerator	Otorga permiso para eliminar un moderador de canal	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteDelegate	Otorga permiso para eliminar la Cuenta de AWS administración delegada de su cuenta de Amazon Chime	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDomain	Otorga permiso para eliminar un dominio de la cuenta de Amazon Chime.	Write			
DeleteEventsConfiguration	Otorga permiso para eliminar una configuración de eventos para que un bot reciba eventos de salida.	Write			
DeleteGroups	Otorga permiso para eliminar grupos de usuarios de Active Directory u Okta de su cuenta de Amazon Chime Enterprise.	Write			
DeleteMediaCapturePipeline	Otorga permiso para eliminar una canalización de captura multimedia.	Escritura	media-pipeline*		
DeleteMediaInsightsPipelineConfiguration	Concede permiso para eliminar una configuración de canalización de información multimedia	Escritura	media-insights-pipeline-configuration*		chime:ListVoiceConnectors
DeleteMediaPipeline	Otorga permiso para eliminar una canalización multimedia	Escritura	media-pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMediaPipelineKinesisVideoStreamPool	Concede permiso para eliminar un grupo de transmisiones de vídeo de Kinesis	Escritura	media-pipeline-kinesis-video-stream-pool*		
DeleteMeeting	Otorga permisos para eliminar la reunión de Amazon Chime SDK especificada	Escritura	meeting*		
DeleteMessagingStreamingConfigurations	Otorga permiso para eliminar las configuraciones de transmisión de datos de un AppInstance	Escritura	app-instance*		
DeletePhoneNumber	Otorga permiso para mover un número de teléfono a la cola de eliminación.	Write			
DeleteProxySession	Otorga permiso para eliminar una sesión de proxy para el Amazon Chime Voice Connector especificado	Write	voice-connector*		
DeleteRoom	Otorga permisos para eliminar una sala	Write			
DeleteRoomMembership	Otorga permisos para eliminar un miembro de sala	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSipMediaApplication	Otorga permiso para eliminar la aplicación multimedia SIP Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	sip-media-application*		
DeleteSipRule	Otorga permiso para eliminar la regla SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura			
DeleteVoiceConnector	Otorga permiso para eliminar el Amazon Chime Voice Connector especificado.	Write	voice-connector*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
DeleteVoiceConnectorEmergencyCallingConfiguration	Otorga permiso para eliminar la configuración de llamada de emergencia para el Amazon Chime Voice Connector especificado	Escritura	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteVoiceConnectorExternalSystemsConfiguration	Otorga permiso para eliminar la configuración del sistema externo que está conectado al conector de voz Amazon Chime especificado	Escritura	voice-connector*		
DeleteVoiceConnectorGroup	Otorga permiso para eliminar el grupo de Amazon Chime Voice Connector especificado.	Write			
DeleteVoiceConnectorOrigination	Otorga permiso para eliminar la configuración de origen del Amazon Chime Voice Connector especificado.	Write	voice-connector*		
DeleteVoiceConnectorProxy	Otorga permiso para eliminar la configuración de proxy para el Amazon Chime Voice Connector especificado.	Write	voice-connector*		
DeleteVoiceConnectorStreamingConfiguration	Otorga permiso para eliminar la configuración de streaming para el Amazon Chime Voice Connector especificado.	Write	voice-connector*		
DeleteVoiceConnectorTermination	Otorga permiso para eliminar la configuración de terminación del Amazon Chime Voice Connector especificado.	Write	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteVoiceConnectorTerminationCredentials	Otorga permiso para eliminar las credenciales de terminación SIP del Amazon Chime Voice Connector especificado.	Escritura	voice-connector*		
DeleteVoiceProfile	Concede permiso para eliminar un perfil de voz	Escritura	voice-profile*		
DeleteVoiceProfileDomain	Concede permiso para eliminar un dominio de perfil de voz	Escritura	voice-profile-domain*		
DeregisterAppInstanceUserEndpoint	Otorga permiso para anular el registro de un punto de conexión para un usuario de instancia de aplicaciones.	Escritura	app-instance-user*		
DescribeAppInstance	Otorga permiso para obtener todos los detalles de un AppInstance	Lectura	app-instance*		
DescribeAppInstanceAdmin	Otorga permiso para obtener todos los detalles de un AppInstanceAdmin	Lectura	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DescribeAppInstanceBot	Otorga permiso para obtener todos los detalles de un AppInstanceBot	Lectura	app-instance-bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAppInstanceUser	Otorga permiso para obtener todos los detalles de un AppInstanceUser	Lectura	app-instance-user*		
DescribeAppInstanceUserEndpoint	Otorga permiso para describir un punto de conexión registrado para un usuario de instancia de aplicaciones.	Lectura	app-instance-user*		
DescribeChannel	Otorga permiso para obtener los detalles completos de un canal	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelBan	Otorga permiso para obtener los detalles completos de una prohibición de canal	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelFlow	Otorga el permiso para obtener los detalles completos de un flujo de canal	Lectura	channel-flow*		
DescribeChannelMembership	Otorga permiso para obtener los detalles completos de una membresía de canal	Lectura	app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channel*		
DescribeChannelMembershipForAppInstanceUser	Concede permiso para obtener los detalles de un canal en función de la pertenencia del usuario o bot especificado	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModeratedByAppInstanceUser	Concede permiso para obtener los detalles completos de un canal moderado por el usuario o bot especificado	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModerator	Otorga permiso para obtener todos los detalles de una sola ChannelModerator	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
DisassociateChannelFlow	Otorga el permiso para desasociar un flujo de un canal.	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channel-flow*		
DisassociatePhoneNumberFromUser	Otorga permiso para desasociar el número de teléfono aprovisionado principal del usuario de Amazon Chime especificado.	Write			
DisassociatePhoneNumbersFromVoiceConnector	Otorga permiso para desasociar varios números de teléfono del Amazon Chime Voice Connector especificado.	Write	voice-connector*		
DisassociatePhoneNumbersFromVoiceConnectorGroup	Otorga permiso para desasociar varios números de teléfono del grupo de Amazon Chime Voice Connector especificado.	Escritura			
DisassociateSigninDelegateGroupsFromAccount	Otorga permiso para desvincular los grupos de delegados de inicio de sesión especificados de la cuenta de Amazon Chime especificada.	Escritura			
DisassociateVoiceConnectorConnect [solo permiso]	Otorga permiso para desasociar la instancia de Amazon Connect del conector de voz de Amazon Chime especificado	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisconnectDirectory	Otorga permiso para desconectar el servicio de Active Directory de su cuenta de Amazon Chime Enterprise.	Write			
GetAccount	Otorga permiso para obtener información de la cuenta de Amazon Chime especificada.	Read			
GetAccountResource	Otorga permiso para obtener información del recurso de la cuenta asociada con su cuenta de Amazon Chime.	Read			
GetAccountSettings	Otorga permiso para obtener la configuración de la cuenta del ID de la cuenta de Amazon Chime especificado.	Lectura			
GetAccountWithOpenIdConfig	Otorga permiso para obtener los detalles y OpenIdConfig los atributos de la cuenta de Amazon Chime	Lectura			
GetAppInstanceRetentionSettings	Otorga permiso para obtener la configuración de retención de una instancia de aplicaciones	Read	app-instance*		
GetAppInstanceStreamingConfigurations	Otorga permiso para obtener las configuraciones de streaming de una instancia de aplicaciones	Read	app-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAttendee	Otorga permisos para obtener los detalles del asistente para un ID de reunión y un ID de asistente especificados	Read	meeting*		
GetBot	Otorga permiso para recuperar la información del bot especificado.	Read			
GetCDRBucket	Otorga permiso para obtener los detalles de un bucket de S3 de registro de detalles de llamadas asociado a su cuenta de Amazon Chime.	Lectura			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite
GetChannelMembershipPreferences	Otorga permiso para obtener las preferencias de una membresía de canal.	Lectura	app-instance-bot* app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channel*		
GetChannelMessage	Otorga permiso para obtener los detalles completos de un mensaje de canal	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessageStatus	Otorga el permiso para obtener el estado de un mensaje de canal	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
GetDomain	Otorga permiso para obtener detalles de un dominio asociado a su cuenta de Amazon Chime.	Read			
GetEventsConfiguration	Otorga permiso para recuperar información de una configuración de eventos para que un bot reciba eventos de salida.	Lectura			
GetGlobalSettings	Otorga permiso para obtener la configuración global relacionada con Amazon Chime para Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMediaCapturePipeline	Otorga permiso para obtener una canalización de captura multimedia existente.	Lectura	media-pipeline*		
GetMediaInsightsPipelineConfiguration	Concede permiso para obtener una configuración de canalización de información multimedia	Lectura	media-insights-pipeline-configuration*		
GetMediaPipeline	Otorga permiso para obtener una canalización multimedia existente	Lectura	media-pipeline*		
GetMediaPipelineKinesisVideoStreamPool	Otorga permiso para obtener una canalización multimedia existente	Lectura	media-pipeline-kinesis-video-stream-pool*		
GetMeeting	Otorga permisos para obtener el registro de reunión de un ID de reunión especificado	Read	meeting*		
GetMeetingDetail	Otorga permiso para obtener el asistente, la conexión y otros datos de una reunión.	Read			
GetMessagingSessionEndpoint	Otorga permiso para obtener el punto de enlace de la sesión de mensajería	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMessagingStreamingConfigurations	Otorga permiso para obtener las configuraciones de transmisión de datos de un AppInstance	Lectura	app-instance*		
GetPhoneNumber	Otorga permiso para obtener información del número de teléfono especificado.	Read			
GetPhoneNumberOrder	Otorga permiso para obtener información del pedido de números de teléfono especificado.	Lectura			
GetPhoneNumberSettings	Otorga permiso para obtener la configuración del número de teléfono relacionada con Amazon Chime para Cuenta de AWS	Lectura			
GetProxySession	Otorga permiso para obtener detalles de la sesión de proxy streaming del Amazon Chime Voice Connector especificado.	Lectura	voice-connector*		
GetRetentionSettings	Otorga permiso para recuperar la configuración de la cuenta de Amazon Chime especificada.	Lectura			
GetRoom	Otorga permisos para recuperar una sala	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSipMediaApplication	Otorga permiso para obtener detalles de la aplicación multimedia SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Lectura	sip-media-application*		
GetSipMediaApplicationAlexaSkillConfiguration	Otorga permiso para obtener los ajustes de configuración de Alexa Skill para la aplicación multimedia SIP Amazon Chime en manos del administrador Cuenta de AWS	Lectura	sip-media-application*		
GetSipMediaApplicationLoggingConfiguration	Otorga permiso para obtener los ajustes de configuración de registro para la aplicación multimedia SIP Amazon Chime bajo la dirección del administrador Cuenta de AWS	Lectura	sip-media-application*		
GetSipRule	Otorga permiso para obtener detalles de la regla SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Lectura			
GetSpeakerSearchTask	Concede permiso para obtener una tarea de búsqueda de locutor en el recurso de Amazon Chime especificado	Lectura	media-pipeline		
			voice-connector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTelephonyLimits	Otorga permiso para obtener los límites de telefonía para el Cuenta de AWS	Lectura			
GetUser	Otorga permiso para obtener información del ID de usuario especificado.	Read			
GetUserActivityReportData	Otorga permiso para mostrar un resumen de la actividad del usuario en la página de detalles del usuario.	Read			
GetUserByEmail	Otorga permiso para obtener los datos de un usuario de Amazon Chime en función de la dirección de correo electrónico en la cuenta de Amazon Chime Enterprise o Team.	Read			
GetUserSettings	Otorga permiso para obtener la configuración de usuario relacionada con el usuario de Amazon Chime especificado.	Read			
GetVoiceConnector	Otorga permiso para obtener información del Amazon Chime Voice Connector especificado.	Read	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVoiceConnectorEmergencyCallingConfiguration	Otorga permiso para obtener detalles de la configuración de llamada de emergencia para el Amazon Chime Voice Connector especificado	Lectura	voice-connector*		
GetVoiceConnectorExternalSystemsConfiguration	Otorga permiso para obtener la configuración del sistema externo que está conectado al conector de voz Amazon Chime especificado	Lectura	voice-connector*		
GetVoiceConnectorGroup	Otorga permiso para obtener detalles del grupo de Amazon Chime Voice Connector especificado.	Read			
GetVoiceConnectorLoggingConfiguration	Otorga permiso para obtener detalles de la configuración de registro del Amazon Chime Voice Connector especificado.	Read	voice-connector*		
GetVoiceConnectorOrigination	Otorga permiso para obtener información de la configuración de origen del Amazon Chime Voice Connector especificado.	Read	voice-connector*		
GetVoiceConnectorProxy	Otorga permiso para obtener detalles de la configuración de proxy del Amazon Chime Voice Connector especificado.	Read	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVoiceConnectorStreamingConfiguration	Otorga permiso para obtener detalles de la configuración de streaming del Amazon Chime Voice Connector especificado.	Read	voice-connector*		
GetVoiceConnectorTermination	Otorga permiso para obtener información de la configuración de terminación del Amazon Chime Voice Connector especificado.	Read	voice-connector*		
GetVoiceConnectorTerminationHealth	Otorga permiso para obtener información del estado de terminación del Amazon Chime Voice Connector especificado.	Lectura	voice-connector*		
GetVoiceProfile	Concede permiso para obtener un perfil de voz	Lectura	voice-profile*		
GetVoiceProfileDomain	Concede permiso para obtener un dominio de perfil de voz	Lectura	voice-profile-domain*		
GetVoiceToneAnalysisTask	Concede permiso para obtener una tarea de análisis de tono de voz en el recurso de Amazon Chime especificado	Lectura	media-pipeline voice-connector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InviteDelegate	Otorga permiso para enviar una invitación a aceptar una solicitud de Cuenta de AWS delegación para una cuenta de Amazon Chime	Escritura			
InviteUsers	Otorga permiso para invitar hasta a 50 usuarios a la cuenta de Amazon Chime especificada.	Write			
InviteUsersFromProvider	Otorga permiso para invitar a usuarios de un proveedor externo a la cuenta de Amazon Chime.	Write			
ListAccountUsageReportData	Otorga permiso para mostrar los datos del informe de uso de la cuenta de Amazon Chime.	Enumeración			
ListAccounts	Otorga permiso para incluir las cuentas de Amazon Chime en la del administrador Cuenta de AWS	Enumeración			
ListApiKeys	Otorga permiso para mostrar las claves de acceso SCIM definidas para su cuenta de Amazon Chime y configuración de Okta.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAppInstanceAdmins	Otorga permiso para enumerar los administradores de la instancia de aplicaciones	Enumeración	app-instance*		
			app-instance-bot*		
			app-instance-user*		
ListAppInstanceBots	Otorga permiso para enumerar todo lo AppInstanceBots creado en una sola instancia de aplicación	Enumeración	app-instance-bot*		
ListAppInstanceUserEndpoints	Otorga permiso para enumerar los puntos de conexión registrados para un usuario de instancia de aplicaciones.	Enumeración	app-instance-user*		
ListAppInstanceUsers	Otorga permiso para enumerar todo lo AppInstanceUsers creado en una sola instancia de aplicación	Enumeración	app-instance-user*		
ListAppInstances	Otorga permiso para enumerar todas las instancias de la aplicación Amazon Chime creadas en una sola Cuenta de AWS	Enumeración	app-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAttendeeTags	Otorga permiso para enumerar las etiquetas aplicadas a un recurso de asistente de Amazon Chime SDK	List	meeting*		
ListAttendees	Otorga permisos para apuntar hasta 100 asistentes a una reunión específica de Amazon Chime SDK	Enumeración	meeting*		
ListAvailableVoiceConnectorRegions	Otorga permiso para enumerar los conectores de Regiones de AWS voz disponibles en los que puede crear un conector de voz del SDK de Amazon Chime	Enumeración			
ListBots	Otorga permiso para mostrar los bots asociados con la cuenta de Amazon Chime Enterprise del administrador.	List			
ListCDRBucket	Otorga permiso para obtener una lista de buckets de S3 de registro de detalles de llamadas.	Enumeración			s3:ListAllMyBuckets s3:ListBucket

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCallingRegions	Otorga permiso para enumerar las regiones de llamadas disponibles para el administrador Cuenta de AWS	Enumeración			
ListChannelBans	Concede permiso para enumerar todos los usuarios y bots prohibidos en un canal determinado	Enumeración	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelFlows	Otorga permiso para enumerar todos los flujos de canales creados con una sola campanilla AppInstance	Enumeración	channel-flow*		
ListChannelMemberships	Otorga permiso para enumerar todas las membresías de un canal	Enumeración	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelMembershipsForAppInstanceUser	Concede permiso para enumerar todos los canales de los que un usuario o bot determinado forma parte	Enumeración	app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListChannelMessages	Otorga permiso para enumerar todos los mensajes de un canal	Lectura	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelModerators	Otorga permiso para enumerar todos los moderadores de un canal	Enumeración	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannels	Otorga permiso para enumerar todos los canales creados con un solo timbre AppInstance	Enumeración	app-instance-bot*		
			app-instance-user*		
ListChannelsAssociatedWithChannelFlow	Otorga permiso para enumerar todos los canales asociados a un único canal de flujo de Chime	Enumeración	channel-flow*		
ListChannelsModeratedByAppInstanceUser	Concede permiso para enumerar todos los canales moderados por un usuario o bot	Enumeración	app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDelegates	Otorga permiso para mostrar la información de delegación de la cuenta correspondiente a su cuenta de Amazon Chime.	Enumeración			
ListDirectories	Otorga permiso para enumerar los Active Directories activos alojados en el Directory Service de su Cuenta de AWS	Enumeración			
ListDomains	Otorga permiso para mostrar los dominios asociados a su cuenta de Amazon Chime.	List			
ListGroups	Otorga permiso para mostrar los grupos de usuarios de Active Directory u Okta asociados a cuenta de Amazon Chime Enterprise.	List			
ListMediaCapturePipelines	Otorga permiso para enumerar canalizaciones de captura multimedia.	Enumeración			
ListMediaInsightsPipelineConfigurations	Concede permiso para enumerar todas las configuraciones de canalización de información multimedia	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMediaPipelineKinesisVideoStreamPools	Otorga permiso para enumerar canalizaciones multimedia	Enumeración			
ListMediaPipelines	Otorga permiso para enumerar canalizaciones multimedia	Enumeración			
ListMeetingEvents	Otorga permiso para mostrar todos los eventos que han tenido lugar para una reunión especificada.	Enumeración			
ListMeetingTags	Otorga permiso para enumerar las etiquetas aplicadas a un recurso de reunión de Amazon Chime SDK	Enumeración	meeting*		
ListMeetings	Otorga permisos para publicar hasta 100 reuniones activas de Amazon Chime SDK	List			
ListMeetingsReportData	Otorga permiso para mostrar las reuniones finalizadas durante el intervalo de tiempo especificado.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPhoneNumberOrders	Otorga permiso para incluir los pedidos de números de teléfono bajo la dirección del administrador Cuenta de AWS	Enumeración			
ListPhoneNumbers	Otorga permiso para incluir los números de teléfono en la lista del administrador Cuenta de AWS	Enumeración			
ListProxySessions	Otorga permiso para publicar sesiones de proxy para el Amazon Chime Voice Connector especificado	List	voice-connector*		
ListRoomMemberships	Otorga permisos para enumerar todos los miembros de la sala	List			
ListRooms	Otorga permisos para enumerar salas	Enumeración			
ListSipMediaApplications	Otorga permiso para publicar todas las aplicaciones multimedia SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Enumeración			
ListSipRules	Otorga permiso para enumerar todas las reglas SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Enumeración	sip-media-application		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSubChannels	Otorga permiso para enumerarlas todas SubChannels en un solo canal	Enumeración	app-instance-bot*		
			app-instance-user*		
			channel*		
ListSupportedPhoneNumberCountries	Otorga permiso para incluir los números de teléfono de los países admitidos por Cuenta de AWS	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas aplicadas a un recurso de Amazon Chime	Lectura	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		
ListUsers	Otorga permiso para mostrar los usuarios que pertenecen a la cuenta de Amazon Chime especificada.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListVoiceConnectorGroups	Otorga permiso para incluir los grupos de conectores de voz de Amazon Chime en la lista del administrador Cuenta de AWS	Enumeración			
ListVoiceConnectorTerminationCredentials	Otorga permiso para obtener la lista de las credenciales de terminación SIP del Amazon Chime Voice Connector especificado.	Enumeración	voice-connector*		
ListVoiceConnectors	Otorga permiso para incluir los conectores de voz de Amazon Chime en la lista del administrador Cuenta de AWS	Enumeración			
ListVoiceProfileDomains	Concede permiso para enumerar dominios de perfil de voz	Enumeración			
ListVoiceProfiles	Concede permiso para enumerar perfiles de voz	Enumeración	voice-profile-domain*		
LogoutUser	Otorga permiso para cerrar la sesión del usuario especificado de todos los dispositivos a los que está conectado actualmente.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutAppInstanceRetentionSettings	Otorga permiso para habilitar la retención de datos en la instancia de aplicaciones	Write	app-instance*		
PutAppInstanceStreamingConfigurations	Otorga permiso para configurar el streaming de datos de la instancia de aplicaciones	Escritura	app-instance*		
PutAppInstanceUserExpirationSettings	Otorga permiso para establecer la configuración de caducidad de un AppInstanceUser	Escritura	app-instance-user*		
PutChannelExpirationSettings	Concede permiso para poner configuración de vencimiento para un canal	Escritura	app-instance-user*		
			channel*		
PutChannelMembershipPreferences	Otorga permiso para establecer las preferencias de una membresía de canal.	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
PutEventsConfiguration	Otorga permiso para actualizar la información de una configuración de eventos para que un bot reciba eventos de salida.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutMessagingStreamingConfigurations	Otorga permiso para colocar las configuraciones de transmisión de datos de un AppInstance	Escritura	app-instance*		
PutRetentionSettings	Otorga permiso para crear o actualizar la configuración de retención de la cuenta de Amazon Chime especificada	Escritura			
PutSipMediaApplicationAlexaSkillConfiguration	Otorga permiso para actualizar los ajustes de configuración de Alexa Skill para la aplicación multimedia SIP Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	sip-media-application*		
PutSipMediaApplicationLoggingConfiguration	Otorga permiso para actualizar los ajustes de configuración de registro de la aplicación multimedia SIP Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	sip-media-application*		
PutVoiceConnectorEmergencyCallingConfiguration	Otorga permiso para agregar la configuración de llamada de emergencia del Amazon Chime Voice Connector especificado	Escritura	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutVoiceConnectorExternalSystemsConfiguration	Otorga permiso para actualizar la configuración del sistema externo que está conectado al conector de voz Amazon Chime especificado	Escritura	voice-connector*		
PutVoiceConnectorLoggingConfiguration	Otorga permiso para agregar la configuración de registro del Amazon Chime Voice Connector especificado.	Write	voice-connector*		logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutVoiceConnectorOrigination	Otorga permiso para actualizar la configuración de origen del Amazon Chime Voice Connector especificado.	Write	voice-connector*		
PutVoiceConnectorProxy	Otorga permiso para agregar la configuración de proxy del Amazon Chime Voice Connector especificado.	Write	voice-connector*		
PutVoiceConnectorStreamingConfiguration	Otorga permiso para agregar la configuración de streaming del Amazon Chime Voice Connector especificado.	Write	voice-connector*		chime:GetMediaInsightsPipelineConfiguration
			media-insights-pipeline-configuration		
PutVoiceConnectorTermination	Otorga permiso para actualizar la configuración de terminación del Amazon Chime Voice Connector especificado.	Write	voice-connector*		
PutVoiceConnectorTerminationCredentials	Otorga permiso para agregar las credenciales de terminación SIP del Amazon Chime Voice Connector especificado.	Write	voice-connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RedactChannelMessage	Otorga permiso para redactar el contenido del mensaje	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
RedactConversationMessage	Otorga permiso para redactar el mensaje de conversación de Chime especificado	Escritura			
RedactRoomMessage	Otorga permiso para redactar el mensaje de la sala de Chime especificado	Escritura			
RegenerateSecurityToken	Otorga permiso para regenerar el token de seguridad del bot especificado.	Escritura			
RegisterAppInstanceUserEndpoint	Otorga permiso para registrar un punto de conexión para un usuario de instancia de aplicaciones.	Escritura	app-instance-user*		mobiletargeting:GetApp
RenameAccount	Otorga permiso para modificar el nombre de cuenta de Amazon Chime Enterprise o Team.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RenewDelegate	Otorga permiso para renovar la solicitud de delegación asociada a una cuenta de Amazon Chime.	Write			
ResetAccountResource	Otorga permiso para restablecer el recurso en su cuenta de Amazon Chime.	Write			
ResetPersonalPIN	Otorga permiso para restablecer el PIN de reunión personal del usuario especificado en una cuenta de Amazon Chime.	Write			
RestorePhoneNumber	Otorga permiso para restaurar el número de teléfono especificado de la cola de eliminación en el inventario de números de teléfono.	Write			
RetrieveDataExports	Otorga permiso para descargar el archivo que contiene los enlaces a todos los archivos adjuntos de los usuarios que se devuelven como parte de la acción de solicitar archivos adjuntos.	Lectura			
SearchAvailablePhoneNumbers	Otorga permiso para buscar números de teléfono que pueden solicitarse al operador.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchChannels	Otorga permiso para buscar en los canales a los que AppInstanceUser pertenece una persona o buscar en los canales que estén en el AppInstance mismo AppInstaceAdmin	Enumeración	app-instance-bot*		
			app-instance-user*		
SendChannelMessage	Otorga permiso para enviar un mensaje a un canal particular del que el miembro forma parte	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
StartDataExport	Otorga permiso para enviar la solicitud de solicitar archivos adjuntos.	Escritura			
StartMeetingTranscription	Otorga permiso para comenzar la transcripción de una reunión	Escritura			
StartSpeakerSearchTask	Concede permiso para iniciar una tarea de búsqueda de locutor en el recurso de Amazon Chime especificado	Escritura	media-pipeline		
			voice-connector		
StartVoiceToneAnalysisTask	Concede permiso para iniciar una tarea de análisis de tono de voz en el recurso de Amazon Chime especificado	Escritura	media-pipeline		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			voice-connector		
StopMeetingTranscription	Otorga permiso para detener la transcripción de una reunión	Escritura			
StopSpeakerSearchTask	Concede permiso para detener una tarea de búsqueda de locutor en el recurso de Amazon Chime especificado	Escritura	media-pipeline		
			voice-connector		
StopVoiceToneAnalysisTask	Concede permiso para detener una tarea de análisis de tono de voz en el recurso de Amazon Chime especificado	Escritura	media-pipeline		
			voice-connector		
SubmitSupportRequest	Otorga permiso para enviar una solicitud de soporte al servicio de atención al cliente.	Write			
SuspendUsers	Otorga permiso para suspender a los usuarios de una cuenta de Amazon Chime Enterprise.	Write			
TagAttendee	Otorga permiso para aplicar las etiquetas especificadas al asistente de Amazon Chime SDK especificado	Etiquetado	meeting*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagMeeting	Otorga permiso para aplicar las etiquetas especificadas a la reunión de Amazon Chime SDK especificada	Etiquetado	meeting*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para aplicar las etiquetas especificadas al recurso especificado (los controles de acceso basados en etiquetas solo se admiten en los puntos de conexión *-chime.<region>.amazonaws.com)	Etiquetado	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UnauthorizeDirectory	Otorga permiso para desautorizar un servicio de Active Directory de su cuenta de Amazon Chime Enterprise.	Escritura			
UntagAttendee	Otorga permiso para desetiquetar las etiquetas especificadas del asistente de Amazon Chime SDK especificado	Etiquetado	meeting*		
UntagMeeting	Otorga permiso para desetiquetar las etiquetas especificadas de la reunión de Amazon Chime SDK especificada	Etiquetado	meeting*		
UntagResource	Concede permiso para quitar las etiquetas especificadas del recurso especificado (los controles de acceso basados en etiquetas solo se admiten en los puntos de conexión *-chime.<region>.amazonaws.com)	Etiquetado	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccount	Otorga permiso para actualizar los detalles de la cuenta de Amazon Chime especificada.	Escritura			
UpdateAccountOpenIdConfig	Otorga permiso para actualizar los OpenIdConfig atributos de su cuenta de Amazon Chime	Escritura			
UpdateAccountResource	Otorga permiso para actualizar el recurso de la cuenta de Amazon Chime.	Write			
UpdateAccountSettings	Otorga permiso para actualizar la configuración de la cuenta de Amazon Chime especificada.	Escritura			
UpdateAppInstance	Otorga permiso para actualizar los metadatos AppInstance	Escritura	app-instance*		
UpdateAppInstanceBot	Otorga permiso para actualizar los detalles de un AppInstanceBot	Escritura	app-instance-bot*		
UpdateAppInstanceUser	Otorga permiso para actualizar los detalles de un AppInstanceUser	Escritura	app-instance-user*		
UpdateAppInstanceUserEndpoint	Otorga permiso para actualizar un punto de conexión registrado para un usuario de instancia de aplicaciones.	Escritura	app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAttendeeCapabilities	Otorga permiso para las capacidades que desea actualizar.	Escritura	meeting*		
UpdateBot	Otorga permiso para actualizar el estado del bot especificado.	Write			
UpdateCDRSettings	Otorga permiso para actualizar el bucket de S3 de registro de detalles de llamadas.	Write			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets
UpdateChannel	Otorga permiso para actualizar los atributos de un canal	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelFlow	Otorga el permiso para actualizar un flujo de canal	Escritura	channel-flow*		
UpdateChannelMessage	Otorga permiso para actualizar el contenido de un mensaje	Write	app-instance-bot*		
			app-instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			channel*		
UpdateChannelReadMarker	Otorga permiso para establecer la marca temporal en el punto en que un usuario leyó por última vez los mensajes de un canal	Escritura	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateGlobalSettings	Otorga permiso para actualizar la configuración global relacionada con Amazon Chime para Cuenta de AWS	Escritura			
UpdateMediaInsightsPipelineConfiguration	Concede permiso para actualizar el estado de una configuración de canalización de información multimedia	Escritura	media-insights-pipeline-configuration*		chime:ListVoiceConnectors iam:PassRole kinesis:DescribeStream s3:ListBucket
UpdateMediaInsightsPipelineStatus	Concede permiso para actualizar el estado de una canalización de información multimedia	Escritura	media-pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMediaPipelineKinesisVideoStreamPool	Concede permiso para actualizar un grupo de transmisiones de vídeo de Kinesis	Escritura	media-pipeline-kinesis-video-stream-pool*		
UpdatePhoneNumber	Otorga permiso para actualizar la información del número de teléfono especificado.	Escritura			
UpdatePhoneNumberSettings	Otorga permiso para actualizar la configuración del número de teléfono relacionada con Amazon Chime para Cuenta de AWS	Escritura			
UpdateProxySession	Otorga permiso para actualizar una sesión proxy para el Amazon Chime Voice Connector especificado	Write	voice-connector*		
UpdateRoom	Otorga permisos para actualizar una sala	Write			
UpdateRoomMembership	Otorga permisos para actualizar el rol de pertenencia a la sala	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSipMediaApplication	Otorga permiso para actualizar las propiedades de la aplicación multimedia SIP Amazon Chime bajo la supervisión del administrador Cuenta de AWS	Escritura	sip-media-application*		
UpdateSipMediaApplicationCall	Otorga permiso para actualizar una llamada a una aplicación multimedia SIP de Amazon Chime bajo la dirección del administrador Cuenta de AWS	Escritura	sip-media-application*		
UpdateSipRule	Otorga permiso para actualizar las propiedades de la regla SIP de Amazon Chime según la regla del administrador Cuenta de AWS	Escritura	sip-media-application		
UpdateSupportedLicenses	Otorga permiso para actualizar los niveles de licencia compatibles disponibles para los usuarios en su cuenta de Amazon Chime.	Write			
UpdateUser	Otorga permiso para actualizar los detalles del usuario de un ID de usuario especificado.	Write			
UpdateUserLicenses	Otorga permiso para actualizar las licencias de los usuarios de Amazon Chime.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateUserSettings	Otorga permiso para actualizar la configuración de usuario relacionada con el usuario de Amazon Chime especificado.	Write			
UpdateVoiceConnector	Otorga permiso para actualizar los detalles del Amazon Chime Voice Connector para el Amazon Chime Voice Connector especificado.	Write	voice-connector*		
UpdateVoiceConnectorGroup	Otorga permiso para actualizar los detalles del grupo de Amazon Chime Voice Connector del grupo de Amazon Chime Voice Connector especificado.	Escritura	voice-connector		
UpdateVoiceProfile	Concede permiso para actualizar un perfil de voz	Escritura	voice-profile*		
UpdateVoiceProfileDomain	Concede permiso para actualizar un dominio de perfil de voz	Escritura	voice-profile-domain*		
ValidateAccountResource	Otorga permiso para validar el recurso en su cuenta de Amazon Chime.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ValidateE911Address	Otorga permiso para validar una dirección que se utilizará en las llamadas al 911 realizadas con Amazon Chime Voice Connectors	Lectura			

Tipos de recursos definidos por Amazon Chime

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
meeting	`arn:${Partition}:chime::${AccountId}:meeting/${MeetingId}`	aws:ResourceTag/${TagKey}
app-instance	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}`	aws:ResourceTag/${TagKey}
app-instance-user	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/user/${AppInstanceUserId}`	aws:ResourceTag/${TagKey}
app-instance-bot	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/bot/${AppInstanceBotId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
channel	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel/${ChannelId}	aws:ResourceTag/${TagKey}
channel-flow	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel-flow/${ChannelFlowId}	aws:ResourceTag/${TagKey}
media-pipeline	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline/${MediaPipelineId}	aws:ResourceTag/${TagKey}
media-insights-pipeline-configuration	arn:${Partition}:chime:${Region}:${AccountId}:media-insights-pipeline-configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}
media-pipeline-kinesis-video-stream-pool	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline-kinesis-video-stream-pool/${PoolName}	aws:ResourceTag/${TagKey}
voice-profile-domain	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile-domain/${VoiceProfileDomainId}	aws:ResourceTag/${TagKey}
voice-profile	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile/${VoiceProfileId}	
voice-connector	arn:${Partition}:chime:${Region}:${AccountId}:vc/${VoiceConnectorId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
sip-media-application	`arn:${Partition}:chime:${Region}:${AccountId}:sma/${SipMediaApplicationId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Chime

Amazon Chime define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Clean Rooms

AWS Clean Rooms (prefijo de servicio:`cleanrooms`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Clean Rooms
- Tipos de recursos definidos por AWS Clean Rooms
- Claves de condición para AWS Clean Rooms

Acciones definidas por AWS Clean Rooms

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetCollaborationAnalysisTemplate	Concede permiso para ver los detalles de analysisTemplates asociados a la colaboración	Lectura	analysistemplate*		cleanrooms:GetCollaborationAnalysisTemplate
			collaboration*		
BatchGetSchema	Concede permiso para ver los detalles de esquemas	Lectura	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			idmappingtable		
BatchGetSchemaAnalysisRule	Concede permiso para ver las reglas de análisis asociadas a los esquemas	Lectura	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
CreateAnalysisTemplate	Concede permiso para crear una nueva plantilla de análisis	Escritura	analysistemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaboration	Concede permiso para crear una nueva colaboración, un entorno de colaboración de datos compartidos	Escritura	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfiguredAudienceModelAssociation	Concede permiso para vincular un modelo de audiencia configurada con Cleanrooms ML con una colaboración mediante la creación de una nueva asociación	Escritura	configuredaudiencemodelassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	cleanrooms-ml:GetConfiguredAudienceModel cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfiguredTable	Concede permiso para crear una nueva tabla configurada	Escritura	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	athena:GetTableMetadata glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions glue:GetSchemaVersion glue:GetTable glue:GetTables
CreateConfiguredTableAnalysisRule	Concede permiso para crear una regla de análisis para una tabla configurada	Escritura	configuredtable*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfiguredTableAssociation	Concede permiso para vincular una tabla configurada con una colaboración mediante la creación de una nueva asociación	Escritura	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
			configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfiguredTableAssociationAnalysisRule	Concede permiso para crear una regla de análisis para una asociación de tablas configurada	Escritura	configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdMappingTable	Concede permiso para vincular un flujo de trabajo de asignación de ID con una colaboración. Para ello, crea una nueva tabla de asignación de ID	Escritura	idmappingtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdMappingWorkflow
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIdNamespaceAssociation	Concede permiso para vincular un espacio de nombres de ID de resolución de AWS entidades con una colaboración mediante la creación de una nueva asociación	Escritura	idnamespaceassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdNamespace
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMembership	Concede permiso para unirse a colaboraciones mediante la creación de una suscripción	Escritura	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivacyBudgetTemplate	Concede permiso para crear una nueva plantilla de presupuesto para privacidad	Escritura	membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			privacybudgettemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteAnalysisTemplate	Concede permiso para eliminar una plantilla de análisis existente	Escritura	analysistemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCollaboration	Concede permiso para eliminar una colaboración existente	Escritura	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConfiguredAudienceModelAssociation	Concede permisos para eliminar una asociación existente de modelo de audiencia configurada	Escritura	configuredaudiencemodelassociation*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteConfiguredTable	Concede permiso para eliminar una tabla configurada	Escritura	configuredtable*		
DeleteConfiguredTableAnalysisRule	Concede permiso para eliminar una regla de análisis existente	Escritura	configuredtable*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConfiguredTableAssociation	Concede permiso para eliminar una asociación de tabla configurada de una colaboración	Escritura	configuredtableassociation*		
DeleteConfiguredTableAssociationAnalysisRule	Concede permiso para eliminar una regla de análisis de asociación de tablas configurada existente	Escritura	configuredtableassociation*		
DeleteIdMappingTable	Concede permiso para eliminar una tabla de asignación de ID de una colaboración	Escritura	idmappingtable*		entityresolution:DeletePolicyStatement
			membership*		
DeleteIdNamespaceAssociation	Concede permiso para eliminar una asociación de espacio de nombres de ID de una colaboración	Escritura	idnamespaceassociation*		entityresolution:DeletePolicyStatement
			membership*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMember	Concede permiso para eliminar miembros de una colaboración	Escritura	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteMembership	Concede permiso para abandonar las colaboraciones mediante la eliminación de un suscripción	Escritura	membership*		
DeletePrivacyBudgetTemplate	Concede permiso para eliminar una plantilla existente de presupuesto para privacidad	Escritura	privacybudgettemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAnalysisTemplate	Concede permiso para ver los detalles de una plantilla de análisis	Lectura	analysistemplate*		
GetCollaboration	Concede permiso para ver los detalles de una colaboración	Lectura	collaboration*		
GetCollaborationAnalysisTemplate	Concede permiso para ver los detalles de una plantilla de análisis dentro de una colaboración	Lectura	analysistemplate*		
			collaboration*		
GetCollaborationConfiguredAudienceModelAssociation	Concede permiso para ver los detalles de una asociación de modelo de audiencia configurada dentro de una colaboración	Lectura	collaboration*		
			configuredaudiencemodelassociation*		
GetCollaborationIdNamespaceAssociation	Concede permiso para obtener la asociación del espacio de nombres de ID dentro de una colaboración	Lectura	collaboration*		
			idnamespaceassociation*		
GetCollaborationPrivacyBudgetTemplate	Concede permiso para ver los detalles de una plantilla de presupuesto para privacidad dentro de una colaboración	Lectura	collaboration*		
			privacybudgettemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConfiguredAudienceModelAssociation	Concede permiso para ver los detalles para una asociación de modelo configurada	Lectura	configuredaudiencemodelassociation*		
GetConfiguredTable	Concede permiso para ver los detalles de una tabla configurada	Lectura	configuredtable*		
GetConfiguredTableAnalysisRule	Concede permiso para ver las reglas de análisis de una tabla configurada	Lectura	configuredtable*		
GetConfiguredTableAssociation	Concede permiso para ver los detalles de una asociación de tabla configurada	Lectura	configuredtableassociation*		
GetConfiguredTableAssociationAnalysisRule	Concede permiso para ver reglas de análisis de una asociación de tablas configurada	Lectura	configuredtableassociation*		
GetIdMappingTable	Concede permiso para ver los detalles de una tabla de asignación de ID	Lectura	idmappingtable*		
			membership*		
GetIdNamespaceAssociation	Concede permiso para ver los detalles de una asociación de espacio de nombres de ID	Lectura	idnamespaceassociation*		entityresolution:GetIdNamespace

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			membership*		
GetMembership	Concede permiso para ver los detalles de una suscripción	Lectura	membership*		
GetPrivacyBudgetTemplate	Concede permiso para ver los detalles de una plantilla de presupuesto para privacidad	Lectura	privacybudgettemplate*		
GetProtectedJob	Otorga permiso para ver un trabajo protegido	Lectura	membership*		
GetProtectedQuery	Concede permiso para ver una consulta protegida	Lectura	membership*		
GetSchema	Concede permiso para ver los detalles de un esquema	Lectura	collaboration*		
			configuredtableassociation*		
GetSchemaAnalysisRule	Concede permiso para ver las reglas de análisis asociadas a un esquema	Lectura	collaboration*		cleanrooms:GetSchema
			configuredtableassociation*		
ListAnalysisTemplates	Concede permiso para enumerar las plantillas de análisis disponibles	Enumeración	analysistemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			membership*		
ListCollaborationAnalysisTemplates	Concede permiso para enumerar las plantillas de análisis disponibles dentro de una colaboración	Enumeración	collaboration*		
ListCollaborationConfiguredAudienceModelAssociations	Concede permiso para mostrar una lista de las asociaciones de modelos de audiencia configurada disponibles dentro de una colaboración	Enumeración	collaboration*		
ListCollaborationIdNamespaceAssociations	Concede permiso para enumerar el espacio de nombres de ID dentro de una colaboración	Enumeración	collaboration*		
ListCollaborationPrivacyBudgetTemplates	Concede permiso para enumerar las plantillas de presupuesto para privacidad disponibles dentro de una colaboración	Enumeración	collaboration*		
ListCollaborationPrivacyBudgets	Concede permiso para enumerar los presupuestos para privacidad dentro de una colaboración	Enumeración	collaboration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCollaborations	Concede permiso para enumerar las colaboraciones disponibles	Enumeración			
ListConfiguredAudienceModelAssociations	Concede permiso para enumerar las asociaciones de modelo de audiencia configuradas disponibles para una suscripción	Enumeración	configuredaudiencemodelassociation*		
			membership*		
ListConfiguredTableAssociations	Concede permiso para enumerar las asociaciones de tabla configurada disponibles para una suscripción	Enumeración	configuredtableassociation*		
			membership*		
ListConfiguredTables	Concede permiso para enumerar las tablas configuradas disponibles	Enumeración			
ListIdMappingTables	Concede permiso para enumerar las tablas de asignación de ID disponibles para una membresía	Enumeración	idmappingtable*		
			membership*		
ListIdNamespaceAssociations	Concede permiso para enumerar asociaciones de datos de Entity Resolution para una membresía	Enumeración	idnamespaceassociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			membership*		
ListMembers	Concede permiso para enumerar a los miembros de una colaboración	Enumeración	collaboration*		
ListMemberships	Concede permiso para enumerar las suscripciones disponibles	Enumeración			
ListPrivacyBudgetTemplates	Concede permiso para enumerar las plantillas de presupuesto para privacidad disponibles	Enumeración	membership*		
			privacybudgettemplate*		
ListPrivacyBudgets	Concede permiso para enumerar los presupuestos de privacidad disponibles	Enumeración	membership*		
ListProtectedJobs	Otorga permiso para publicar trabajos protegidos	Enumeración	membership*		
ListProtectedQueries	Concede permiso para enumerar las consultas protegidas	Enumeración	membership*		
ListSchemas	Concede permiso para ver los esquemas disponibles para una colaboración	Enumeración	collaboration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	List	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			membership		
			privacybudgettemplate		
PassCollaboration [solo permiso]	Otorga permiso para acceder a una colaboración en el contexto de los modelos personalizados de Clean Rooms ML	Lectura	collaboration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PassMembership [solo permiso]	Otorga permiso para acceder a una membresía en el contexto de los modelos personalizados de Clean Rooms ML	Lectura	membership*		
PopulateIdMappingTable	Otorga permiso para iniciar un trabajo de mapeo de identidad en AWS Entity Resolution a fin de generar resultados de mapeo de identidad en la colaboración de salas limpias.	Escritura	idmappingtable*		entityresolution:GetIdMappingWorkflow
			membership*		
PreviewPrivacyImpact	Otorga permiso para previsualizar la configuración de la plantilla de presupuesto para privacidad	Lectura	membership*		
StartProtectedJob	Otorga permiso para iniciar trabajos protegidos	Escritura	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema
			analysistemplate		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			configuredtableassociation		
StartProtectedQuery	Concede permiso para iniciar consultas protegidas	Escritura	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema s3:GetBucketLocation s3:ListBucket s3:PutObject
			analysistemplate		
			configuredtableassociation		
			idmappingtable		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		
			privacybudgettemplate		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			privacybudgettemplate		
				aws:TagKeys	
UpdateAnalysisTemplate	Concede permiso para actualizar los detalles de la plantilla de análisis	Escritura	analysistemplate*		
UpdateCollaboration	Concede permiso para actualizar los detalles de la colaboración	Escritura	collaboration*		
UpdateConfiguredAudienceModelAssociation	Concede permiso para actualizar una asociación de modelo de audiencia configurada	Escritura	configuredaudiencemodelassociation*		
UpdateConfiguredTable	Concede permiso para actualizar una tabla configurada existente	Escritura	configuredtable*		
UpdateConfiguredTableAnalysisRule	Concede permiso para actualizar las reglas de análisis de una tabla configurada	Escritura	configuredtable*		
UpdateConfiguredTableAssociation	Concede permiso para actualizar una asociación de tabla configurada	Escritura	configuredtableassociation*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConfiguredTableAssociationAnalysisRule	Concede permiso para actualizar las reglas de análisis de una asociación de tablas configurada	Escritura	configuredtableassociation*		
UpdateIdMappingTable	Concede permiso para actualizar una tabla de asignación de ID	Escritura	idmappingtable*		
			membership*		
UpdateIdNamespaceAssociation	Concede permiso para actualizar una asociación de entrada de Entity Resolution	Escritura	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMembership	Concede permiso para actualizar los detalles de una suscripción	Escritura	membership*		iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
UpdatePrivacyBudgetTemplate	Concede permiso para actualizar los detalles de la plantilla de presupuesto para privacidad	Escritura	privacybudgettemplate*		
UpdateProtectedJob	Otorga permiso para actualizar los trabajos protegidos	Escritura	membership*		
UpdateProtectedQuery	Concede permiso para actualizar las consultas protegidas	Escritura	membership*		

Tipos de recursos definidos por AWS Clean Rooms

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
analysistemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/analysistemplate/${AnalysisTemplateId}	aws:ResourceTag/${TagKey}
collaboration	arn:${Partition}:cleanrooms:${Region}:${Account}:collaboration/${CollaborationId}	aws:ResourceTag/${TagKey}
configuredaudiencemodelassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredaudiencemodelassociation/${ConfiguredAudienceModelAssociationId}	aws:ResourceTag/${TagKey}
configuredtable	arn:${Partition}:cleanrooms:${Region}:${Account}:configuredtable/${ConfiguredTableId}	aws:ResourceTag/${TagKey}
configuredtableassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredtableassociation/${ConfiguredTableAssociationId}	aws:ResourceTag/${TagKey}
idmappingtable	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idmappingtable/${IdMappingTableId}	aws:ResourceTag/${TagKey}
idnamespaceassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idnamespaceassociation/${IdNamespaceAssociationId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
membership	`arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}`	aws:ResourceTag/${TagKey}
privacybudgettemplate	`arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/privacybudgettemplate/${PrivacyBudgetTemplateId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Clean Rooms

AWS Clean Rooms define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Clean Rooms ML

AWS Clean Rooms ML (prefijo de servicio:`cleanrooms-ml`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Clean Rooms ML
- Tipos de recursos definidos por AWS Clean Rooms ML
- Claves de condición para AWS Clean Rooms ML

Acciones definidas por AWS Clean Rooms ML

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelTrainedModel	Otorga permiso para cancelar un modelo entrenado	Escritura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelTrainedModelInferenceJob	Otorga permiso para cancelar un trabajo de inferencia de modelos entrenados	Escritura	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAudienceModel	Concede permiso para crear un modelo de audiencia	Escritura	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredAudienceModel	Concede permiso para crear un modelo de audiencia configurado	Escritura	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfiguredModelAlgorithm	Otorga permiso para crear un algoritmo de modelo configurado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredModelAlgorithmAssociation	Otorga permiso para crear una asociación de algoritmos de modelo configurada	Escritura	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMLInputChannel	Otorga permiso para crear un canal de entrada de ML	Escritura	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainedModel	Otorga permiso para crear un modelo entrenado	Escritura	ConfiguredModelAlgorithmAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingDataset	Concede permiso para crear un conjunto de datos de capacitación o audiencia inicial. En Clean Rooms ML, TrainingDataset son los metadatos que apuntan a una tabla de Glue, que solo se lee durante AudienceModel la creación	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceGenerationJob	Otorga permiso para eliminar el trabajo de generación de audiencias especificado y elimina todos los datos asociados al trabajo	Escritura	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceModel	Otorga permiso para eliminar el trabajo de generación de audiencias especificado y elimina todos los datos asociados al trabajo	Escritura	audiencemodel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModel	Otorga permiso para eliminar la configuración del modelo configurado	Escritura	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModelPolicy	Concede permiso para eliminar la política del modelo de audiencia especificada	Escritura	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithm	Otorga permiso para eliminar un algoritmo de modelo configurado	Escritura	ConfiguredModelAlgorithm*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithmAssociation	Otorga permiso para eliminar una asociación de algoritmos de modelo configurada	Escritura	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLConfiguration	Otorga permiso para eliminar una configuración de ML	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLInputChannelData	Otorga permiso para eliminar todos los datos asociados al canal de entrada de ML	Escritura	MLInputChannel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainedModelOutput	Otorga permiso para eliminar todos los resultados asociados al modelo entrenado	Escritura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainingDataset	Concede permiso para eliminar un conjunto de datos de capacitación	Escritura	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceGenerationJob	Concede permiso para devolver información sobre un trabajo de generación de audiencia	Lectura	audiencegenerationjob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceModel	Concede permiso para obtener información acerca de un modelo de audiencia	Lectura	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCollaborationConfiguredModelAlgorithmAssociation	Otorga permiso para devolver información sobre una asociación de algoritmos de modelo configurada creada por cualquier miembro de la colaboración	Lectura	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCollaborationMLInputChannel	Otorga permiso para devolver información sobre un canal de entrada de aprendizaje automático creado por cualquier miembro de la colaboración	Lectura	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetCollaborationTrainedModel	Otorga permiso para devolver información sobre un modelo entrenado creado por cualquier miembro de la colaboración	Lectura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetConfiguredAudienceModel	Otorga permiso para devolver información acerca del modelo de audiencia configurada	Lectura	configuredaudiencemodel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModelPolicy	Concede permiso para devolver información sobre una política de modelo de audiencia configurada	Lectura	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithm	Otorga permiso para devolver información sobre un algoritmo de modelo configurado	Lectura	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithmAssociation	Otorga permiso para devolver información sobre una asociación de algoritmos de modelo configurada	Lectura	ConfiguredModelAlgorithmAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetMLConfiguration	Otorga permiso para devolver información sobre una configuración de ML	Lectura		aws:RequestTag/${TagKey} aws:TagKeys	
GetMLInputChannel	Otorga permiso para devolver información sobre un canal de entrada de ML	Lectura	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModel	Otorga permiso para devolver información sobre un modelo entrenado	Lectura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTrainedModelInferenceJob	Otorga permiso para devolver información sobre un trabajo de inferencia de modelos entrenados	Lectura	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainingDataset	Concede permiso para devolver información sobre un conjunto de datos de capacitación	Lectura	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceExportJobs	Concede permiso para devolver una lista de trabajos de exportación de audiencia	Enumeración	audiencegenerationjob		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAudienceGenerationJobs	Concede permiso para devolver una lista de trabajos de generación de audiencia	Enumeración	configuredaudiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceModels	Otorga permiso para devolver una lista de modelos de audiencia	Enumeración			
ListCollaborationConfiguredModelAlgorithmAssociations	Otorga permiso para devolver una lista de algoritmos de modelo configurados creados por cualquier miembro de la colaboración	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCollaborationMLInputChannels	Otorga permiso para devolver una lista de canales de entrada de aprendizaje automático creados por cualquier miembro de la colaboración	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModelExportJobs	Otorga permiso para devolver una lista de trabajos de exportación de modelos entrenados iniciados por cualquier miembro de la colaboración	Enumeración	TrainedModel*	aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCollaborationTrainedModelInferenceJobs	Otorga permiso para devolver una lista de trabajos de inferencia de modelos entrenados iniciados por cualquier miembro de la colaboración	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModels	Otorga permiso para devolver una lista de modelos entrenados creada por cualquier miembro de la colaboración	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListConfiguredAudienceModels	Otorga permiso para devolver una lista de modelos de audiencia configurada	Enumeración			
ListConfiguredModelAlgorithmAssociations	Otorga permiso para devolver una lista de asociaciones de algoritmos de modelos configuradas	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConfiguredModelAlgorithms	Otorga permiso para devolver una lista de algoritmos de modelo configurados	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListMLInputChannels	Otorga permiso para devolver una lista de canales de entrada de ML	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListTagsForResource	Concede permiso para devolver una lista de etiquetas de un recurso proporcionado	Enumeración	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTrainedModelInferenceJobs	Otorga permiso para devolver una lista de trabajos de inferencia de modelos entrenados	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModels	Otorga permiso para devolver una lista de modelos entrenados	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainingDatasets	Otorga permiso para devolver una lista de conjuntos de datos de capacitación	Enumeración			
PutConfiguredAudienceModelPolicy	Concede permiso para crear o actualizar una política de recursos para un modelo de audiencia configurado	Administración de permisos	configuredaudiencemodel*		
PutMLConfiguration	Otorga permiso para poner una configuración de aprendizaje automático	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceExportJob	Concede permiso para exportar una audiencia de un tamaño específico después de haber generado una audiencia	Escritura	audiencegenerationjob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceGenerationJob	Concede permiso para comenzar el trabajo de generación de audiencia	Escritura	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
StartTrainedModelExportJob	Otorga permiso para iniciar un trabajo de exportación de modelos entrenado	Escritura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartTrainedModelInferenceJob	Otorga permiso para iniciar un trabajo de inferencia de modelos entrenados	Escritura	ConfiguredModelAlgorithmAssociation*		
			MLInputChannel*		
			TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para etiquetar un recurso específico	Etiquetado	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnTagResource	Concede permiso para quitar las etiquetas del recurso específico	Etiquetado	ConfiguredModelAlgorithm		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConfiguredAudienceModel	Concede permiso para actualizar un modelo de audiencia configurado.	Escritura	configuredaudiencemodel*		
			audiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por AWS Clean Rooms ML

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
trainingdataset	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:training-dataset/${ResourceId}	aws:ResourceTag/${TagKey}
audiencemodel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-model/${ResourceId}	aws:ResourceTag/${TagKey}
configuredaudiencemodel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-audience-model/${ResourceId}	aws:ResourceTag/${TagKey}
audiencegenerationjob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-generation-job/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithm	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-model-algorithm/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithmAssociation	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/configured-model-algorithm-association/${ResourceId}	aws:ResourceTag/${TagKey}
MLInputChannel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/ml-input-channel/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model/${ResourceId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
TrainedModelInferenceJob	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model-inference-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Clean Rooms ML

AWS Clean Rooms ML define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
cleanrooms-ml:CollaborationId	Filtra el acceso por identificador de colaboración de salas limpias	Cadena

Claves de condición, acciones y recursos para la API de Nube de AWS Control

Nube de AWS La API de control (prefijo de servicio:`cloudformation`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la API de Nube de AWS Control
- Tipos de recursos definidos por la API de Nube de AWS Control
- Claves de condición para la API de Nube de AWS Control

Acciones definidas por la API de Nube de AWS Control

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelResourceRequest	Otorga permiso para cancelar solicitudes de recursos en su cuenta	Escritura			
CreateResource	Otorga permiso para crear recursos en su cuenta	Escritura			
DeleteResource	Otorga permiso para eliminar recursos de su cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResource	Otorga permiso para obtener recursos en su cuenta	Lectura			
GetResourceRequestStatus	Otorga permiso para obtener solicitudes de recursos en su cuenta	Lectura			
ListResourceRequests	Otorga permiso para enumerar solicitudes de recursos en su cuenta	Lectura			
ListResources	Otorga permiso para enumerar recursos en su cuenta	Lectura			
UpdateResource	Otorga permiso para actualizar recursos en su cuenta	Escritura			

Tipos de recursos definidos por la API de Nube de AWS Control

Nube de AWS La API de control no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la API de Nube de AWS Control, especifique `"Resource": "*"` en su política.

Claves de condición para la API de Nube de AWS Control

La API de Cloud Control no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Cloud Directory

Amazon Cloud Directory (prefijo de servicio: `clouddirectory`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Cloud Directory
- Tipos de recurso definidos por Amazon Cloud Directory
- Claves de condición de Amazon Cloud Directory

Acciones definidas por Amazon Cloud Directory

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddFacetToObject	Concede permiso para agregar una nueva faceta a un objeto	Escritura	directory*		
ApplySchema	Concede permiso para copiar en Directory el esquema de entrada publicado con los mismos nombre y versión que los del esquema publicado	Escritura	directory* publishedSchema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AttachObject	Concede permiso para adjuntar un objeto existente a otro objeto existente	Escritura	directory*		
AttachPolicy	Concede permiso para adjuntar un objeto de política a cualquier otro objeto	Escritura	directory*		
AttachToIndex	Concede permiso para adjuntar el objeto especificado al índice especificado	Escritura	directory*		
AttachTypedLink	Otorga permiso para adjuntar un enlace mecanografiado, b/w una referencia a un objeto de origen y de destino	Escritura	directory*		
BatchRead	Concede permiso para realizar todas las operaciones de lectura de un lote. A cada operación individual interna se le BatchRead deben conceder permisos de forma explícita	Lectura	directory*		
BatchWrite	Concede permiso para realizar todas las operaciones de escritura de un lote. A cada operación individual interna se le BatchWrite deben conceder permisos de forma explícita	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDirectory	Concede permiso para crear un directorio copiando el esquema publicado en el directorio	Escritura	publishedSchema*		
CreateFacet	Concede permiso para crear una nueva faceta en un esquema	Escritura	appliedSchema*		
			developmentSchema*		
CreateIndex	Concede permiso para crear un objeto de índice	Escritura	directory*		
CreateObject	Concede permiso para crear un objeto en un directorio	Escritura	directory*		
CreateSchema	Concede permiso para crear un nuevo esquema en un estado de desarrollo	Escritura			
CreateTypedLinkFacet	Concede permiso para crear una nueva faceta de enlace con tipo en un esquema	Escritura	appliedSchema*		
			developmentSchema*		
DeleteDirectory	Concede permiso para eliminar un directorio. Solo los directorios deshabilitados se pueden eliminar	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFacet	Concede permiso para eliminar una determinada faceta. Todos los atributos y reglas asociados a la faceta se eliminarán	Escritura	developmentSchema*		
DeleteObject	Concede permiso para eliminar un objeto y sus atributos asociados	Escritura	directory*		
DeleteSchema	Concede permiso para eliminar un esquema determinado	Escritura	developmentSchema*		
			publishedSchema*		
DeleteTypedLinkFacet	Otorga permiso para eliminar una TypedLink faceta determinada. Todos los atributos y reglas asociados a la faceta se eliminarán	Escritura	developmentSchema*		
DetachFromIndex	Concede permiso para desconectar el objeto especificado del índice especificado	Escritura	directory*		
DetachObject	Concede permiso para desconectar un objeto determinado del objeto principal	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetachPolicy	Concede permiso para desconectar una política de un objeto	Escritura	directory*		
DetachTypedLink	Otorga permiso para separar un enlace b/w escrito determinado (dada la referencia del objeto de origen y de destino)	Escritura	directory*		
DisableDirectory	Concede permiso para desactivar el directorio especificado	Escritura	directory*		
EnableDirectory	Concede permiso para habilitar el directorio especificado	Escritura	directory*		
GetAppliedSchemaVersion	Concede permiso para devolver el ARN de la versión del esquema aplicado actual, incluida la versión secundaria en uso	Lectura	appliedSchema*		
GetDirectory	Concede permiso para recuperar metadatos sobre un directorio	Lectura	directory*		
GetFacet	Otorga permiso para obtener detalles de la faceta, como el nombre de la faceta, los atributos, las reglas o ObjectType	Lectura	appliedSchema* developmentSchema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			publishedSchema*		
GetLinkAttributes	Concede permiso para recuperar los atributos que están asociados con un enlace con tipo	Lectura	directory*		
GetObjectAttributes	Concede permiso para recuperar los atributos de una faceta que están asociados a un objeto	Lectura	directory*		
GetObjectInformation	Concede permiso para recuperar los metadatos sobre un objeto	Lectura	directory*		
GetSchemaAsJson	Concede permiso para recuperar una representación de JSON del esquema	Lectura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetTypedLinkFacetInformation	Concede permiso para devolver la información del pedido de atributos de identidad asociada a una determinada faceta de enlace con tipo	Lectura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAppliedSchemaArns	Concede permiso para mostrar una lista de los esquemas que se aplican a un directorio	Enumeración	directory*		
ListAttachedIndices	Concede permiso para enumerar los índices adjuntados a un objeto	Lectura	directory*		
ListDevelopmentSchemaArns	Otorga permiso para recuperar ARNs los esquemas en estado de desarrollo	Enumeración			
ListDirectories	Concede permiso para enumerar los directorios creados dentro de una cuenta	Enumeración			
ListFacetAttributes	Concede permiso para recuperar los atributos adjuntados a la faceta	Lectura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListFacetNames	Concede permiso para recuperar los nombres de las facetas que existen en un esquema	Lectura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIncomingTypedLinks	Otorga permiso para devolver una lista paginada de todas las entradas TypedLinks de un objeto determinado	Lectura	directory*		
ListIndex	Concede permiso para enumerar los objetos adjuntados al índice especificado	Lectura	directory*		
ListManagedSchemaArns	Concede permiso para mostrar las familias de versiones principales de cada esquema administrado. Si se proporciona un ARN de la versión principal SchemaArn, en su lugar se muestran las revisiones de la versión secundaria de esa familia.	Enumeración			
ListObjectAttributes	Concede permiso para enumerar todos los atributos asociados a un objeto	Lectura	directory*		
ListObjectChildren	Concede permiso para devolver una lista paginada de los objetos secundarios asociados a un objeto determinado	Lectura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListObjectParentPaths	Concede permiso para recuperar todas las rutas principales disponibles para cualquier tipo de objeto, como objetos de nodo, nodo hijo, nodo de políticas y nodo de índice	Lectura	directory*		
ListObjectParents	Concede permiso para enumerar los objetos principales asociados a un determinado objeto en la forma de paginación	Lectura	directory*		
ListObjectPolicies	Concede permiso para devolver las políticas adjuntadas a un objeto en la forma de paginación	Lectura	directory*		
ListOutgoingTypedLinks	Otorga permiso para devolver una lista paginada de todas las entradas salientes TypedLinks de un objeto determinado	Lectura	directory*		
ListPolicyAttachments	Otorga permiso para devolver todos los elementos ObjectIdentifiers a los que se adjunta una política determinada	Lectura	directory*		
ListPublishedSchemaArns	Otorga permiso para recuperar el esquema publicado ARNs	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para devolver etiquetas para un recurso	Lectura	directory*		
ListTypedLinkFacetAttributes	Concede permiso para devolver una lista paginada de atributos asociados a una faceta de enlace con tipo	Lectura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListTypedLinkFacetNames	Concede permiso para devolver una lista paginada de nombres de una faceta de enlace con tipo que existen en un esquema	Lectura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
LookupPolicy	Concede permiso para enumerar todas las políticas desde la raíz del directorio hasta el objeto especificado	Lectura	directory*		
PublishSchema	Concede permiso para publicar un esquema de desarrollo con una versión	Escritura	developmentSchema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutSchemaFromJson	Concede permiso para actualizar un esquema mediante la carga de JSON. Solo está disponible para esquemas de desarrollo	Escritura			
RemoveFacetFromObject	Concede permiso para quitar la faceta especificada del objeto especificado	Escritura	directory*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	directory*		
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	directory*		
UpdateFacet	Otorga permiso a los atributos, reglas o ObjectType facetas add/update/delete existentes	Escritura	appliedSchema*		
			developmentSchema*		
UpdateLinkAttributes	Concede permiso para actualizar los atributos de un determinado enlace con tipo. Los atributos que se van a actualizar no deben contribuir a la identidad del enlace escrito, tal como lo define su IdentityAttributeOrder	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateObjectAttributes	Concede permiso para actualizar los atributos de un objeto determinado	Escritura	directory*		
UpdateSchema	Concede permiso para actualizar el nombre del esquema con un nuevo nombre	Escritura	developmentSchema*		
UpdateTypedLinkFacet	Otorga permiso a add/update/delete los atributos, las reglas y el orden de los atributos de identidad existentes de una faceta TypedLink	Escritura	developmentSchema*		
UpgradeAppliedSchema	Otorga permiso para actualizar un único directorio in situ utilizando las Published SchemaArn actualizaciones de esquema que se encuentran en. MinorVersion Las actualizaciones de versiones secundarias compatibles con versiones anteriores están disponibles instantáneamente para los lectores en todos los objetos del directorio	Escritura	directory* publishedSchema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpgradePublishedSchema	Otorga permiso para actualizar un esquema publicado con una nueva revisión de la versión secundaria utilizando el contenido actual de DevelopmentSchemaArn	Escritura	developmentSchema*		
			publishedSchema*		

Tipos de recurso definidos por Amazon Cloud Directory

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
appliedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}/schema/${SchemaName}/${Version}`	
developmentSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/development/${SchemaName}`	
directory	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}`	

Tipos de recurso	ARN	Claves de condición
published Schema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}`	

Claves de condición de Amazon Cloud Directory

Cloud Directory no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Nube de AWS Map

Nube de AWS Map (prefijo de servicio:`servicediscovery`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Nube de AWS Map
- Tipos de recursos definidos por Nube de AWS Map
- Claves de condición para Nube de AWS Map

Acciones definidas por Nube de AWS Map

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateHttpNamespace	Otorga permiso para crear un espacio de nombres HTTP.	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	Otorga permiso para crear un espacio de nombres privado basado en DNS, que podrá verse solo dentro de una Amazon VPC especificada.	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePublicDnsNamespace	Otorga permiso para crear un espacio de nombres público basado en DNS, que será visible en Internet.	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Otorga permiso para crear un servicio.	Write	namespace*		
			service*		
				servicediscovery:NamespaceArn aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	
DeleteNamespace	Otorga permiso para eliminar un espacio de nombres específico.	Write	namespace*		
DeleteService	Otorga permiso para eliminar un servicio específico.	Escritura	service*		
DeleteServiceAttributes	Otorga permiso para eliminar atributos específicos de un servicio	Escritura	service*		
DeregisterInstance	Otorga permiso para eliminar los registros y la comprobación de estado, si los hay, que Amazon Route 53 ha creado para la instancia especificada.	Write	service*		
				servicediscovery:ServiceArn	
DiscoverInstances	Otorga permiso para descubrir instancias registradas para un espacio de nombres y servicio especificados.	Lectura		servicediscovery:NamespaceName servicediscovery:ServiceName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DiscoverInstancesRevision	Otorga permiso para descubrir la revisión de las instancias para un espacio de nombres y servicio especificados	Lectura		servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	Otorga permiso para obtener información acerca de una instancia especificada.	Read		servicediscovery:ServiceArn	
GetInstancesHealthStatus	Otorga permiso para obtener el estado actual (Correcto, Incorrecto o Desconocido) de una o más instancias.	Read		servicediscovery:ServiceArn	
GetNamespace	Otorga permiso para obtener información sobre un espacio de nombres.	Read	namespace*		
GetOperation	Otorga permiso para obtener información acerca de una operación especificada.	Read			
GetService	Otorga permiso para obtener la configuración de un servicio especificado.	Lectura	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceAttributes	Otorga permiso para obtener los atributos de un servicio específico	Lectura	service*		
ListInstances	Otorga permiso para obtener información resumida sobre las instancias que se registrar on en un servicio especificado.	Lectura		servicediscovery:ServiceArn	
ListNamespaces	Otorga permiso para obtener información sobre los espacios de nombres.	Lectura			
ListOperations	Otorga permiso para mostrar una lista de operaciones que coincidan con los criterios especificados.	List			
ListServices	Otorga permiso para obtener la configuración de todos los servicios que coincidan con los filtros especificados.	Lectura			
ListTagsForResource	Otorga permiso para mostrar una lista de las etiquetas del recurso especificado.	Lectura			
RegisterInstance	Otorga permiso para registrar una instancia en función de la configuración de un servicio especificado.	Write	service*		
				servicediscovery:ServiceArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar una o más etiquetas al recurso especificado.	Etiquetado		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una o más etiquetas del recurso especificado.	Etiquetado		aws:TagKeys	
UpdateHttpNamespace	Otorga permiso para actualizar la configuración de un espacio de nombres HTTP	Escritura	namespace*		
UpdateInstanceCustomHealthStatus	Otorga permiso para actualizar el estado actual de una instancia que tiene una comprobación de estado personalizada.	Escritura		servicediscovery:ServiceArn	
UpdatePrivateDnsNamespace	Otorga permiso para actualizar la configuración de un espacio de nombres DNS privado	Escritura	namespace*		
UpdatePublicDnsNamespace	Otorga permiso para actualizar la configuración de un espacio de nombres DNS público	Escritura	namespace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateService	Otorga permiso para actualizar la configuración de un servicio especificado.	Escritura	service*		
UpdateServiceAttributes	Otorga permiso para actualizar los atributos de un servicio específico	Escritura	service*		

Tipos de recursos definidos por Nube de AWS Map

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
namespace	`arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
service	`arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}`	aws:ResourceTag/${TagKey}

Claves de condición para Nube de AWS Map

Nube de AWS El mapa define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso.	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se pasan en la solicitud	ArrayOfString
servicediscovery:NamespaceArn	Filtra el acceso especificando el nombre de recurso de Amazon (ARN) para el espacio de nombres relacionado.	ARN
servicediscovery:NamespaceName	Filtra el acceso especificando el nombre del espacio de nombres relacionado.	Cadena
servicediscovery:ServiceArn	Filtra el acceso especificando el nombre de recurso de Amazon (ARN) para el servicio relacionado.	ARN
servicediscovery:ServiceName	Filtra el acceso especificando el nombre del servicio relacionado.	Cadena

Acciones, recursos y claves de condición para AWS Cloud9

AWS Cloud9 (prefijo de servicio:`cloud9`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Cloud9
- Tipos de recursos definidos por AWS Cloud9
- Claves de condición para AWS Cloud9

Acciones definidas por AWS Cloud9

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*).

Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateEC2Remote [solo permiso]	Otorga permiso para iniciar la EC2 instancia de Amazon a la que se AWS conecta tu IDE de Cloud9	Escritura	environment*		
CreateEnvironmentEC2	Otorga permiso para crear un entorno de desarrollo AWS Cloud9, lanza una instancia de Amazon Elastic Compute Cloud EC2 (Amazon) y, a	Escritura		cloud9:EnvironmentName	ec2:DescribeSubnets ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	continuación, aloja el entorno en la instancia			cloud9:InstanceType cloud9:SubnetId cloud9:UserArn cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateEnvironmentMembership	Otorga permiso para añadir un miembro del entorno a un entorno de desarrollo de AWS Cloud9	Escritura	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironmentSSH [solo permiso]	Otorga permiso para crear un entorno de desarrollo SSH en AWS Cloud9	Escritura		cloud9:EnvironmentName cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentToken [solo permiso]	Otorga permiso para crear un token de autenticación que permita una conexión entre el IDE de AWS Cloud9 y el entorno del usuario	Lectura	environment*		
DeleteEnvironment	Otorga permiso para eliminar un entorno de desarrollo de AWS Cloud9. Si el entorno está alojado en una instancia de Amazon Elastic Compute Cloud (Amazon EC2), también termina la instancia	Escritura	environment*		iam:CreateServiceLinkedRole
DeleteEnvironmentMembership	Concede permiso para eliminar un miembro del entorno de un entorno de desarrollo de AWS Cloud9	Escritura	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEC2Remote [solo permiso]	Otorga permiso para obtener detalles sobre la conexión al entorno de EC2 desarrollo, incluidos el host, el usuario y el puerto	Lectura	environment*		
DescribeEnvironmentMemberships	Otorga permiso para obtener información sobre los miembros del entorno para un entorno de desarrollo de AWS Cloud9	Lectura	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEnvironmentStatus	Otorga permiso para obtener información de estado para un entorno de desarrollo de AWS Cloud9	Lectura	environment*		
DescribeEnvironments	Otorga permiso para obtener información sobre los entornos de desarrollo de AWS Cloud9	Lectura	environment*		
DescribeSSHRemote [solo permiso]	Concede permiso para obtener detalles acerca de la conexión al entorno de desarrollo SSH, incluidos el host, el usuario y el puerto	Lectura	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEnvironmentConfig [solo permiso]	Otorga permiso para obtener la información de configuración que se utiliza para inicializar el IDE de AWS Cloud9	Lectura	environment*		
GetEnvironmentSettings [solo permiso]	Otorga permiso para obtener la configuración del IDE de AWS Cloud9 para un entorno de desarrollo específico	Lectura	environment*		
GetMembershipSettings [solo permiso]	Otorga permiso para obtener la configuración del IDE de AWS Cloud9 para un miembro del entorno específico	Lectura	environment*		
GetMigrationExperiences [solo permiso]	Concede permiso para obtener la experiencia de migración de un usuario de Cloud9	Lectura			
GetUserPublicKey [solo permiso]	Otorga permiso para obtener la clave SSH pública del usuario, que AWS Cloud9 utiliza para conectarse a los entornos de desarrollo de SSH	Lectura		cloud9:UserArn	
GetUserSettings [solo permiso]	Otorga permiso para obtener la configuración del IDE de AWS Cloud9 para un usuario específico	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEnvironments	Otorga permiso para obtener una lista de identificadores del AWS entorno de desarrollo de Cloud9	Lectura			
ListTagsForResource	Concede permiso para enumerar etiquetas para un entorno de Cloud9	Lectura	environment*		
ModifyTemporaryCredentialsOnEnvironmentEC2 [solo permiso]	Otorga permiso para establecer credenciales temporales AWS administradas en la EC2 instancia de Amazon que utiliza el entorno de desarrollo integrado (IDE) AWS Cloud9	Escritura	environment*		
TagResource	Concede permiso para agregar etiquetas a un entorno de cloud9	Etiquetado	environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un entorno de cloud9	Etiquetado	environment*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEnvironment	Otorga permiso para cambiar la configuración de un entorno de desarrollo de AWS Cloud9 existente	Escritura	environment*		
UpdateEnvironmentMembership	Otorga permiso para cambiar la configuración de un miembro del entorno existente para un entorno de desarrollo de AWS Cloud9	Escritura	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
UpdateEnvironmentSettings [solo permiso]	Otorga permiso para actualizar la configuración del IDE de AWS Cloud9 para un entorno de desarrollo específico	Escritura	environment*		
UpdateMembershipSettings [solo permiso]	Otorga permiso para actualizar la configuración del IDE de AWS Cloud9 para un miembro del entorno específico	Escritura	environment*		
UpdateSSHRemote [solo permiso]	Concede permiso para actualizar los detalles acerca de la conexión al entorno de desarrollo SSH, incluidos el host, el usuario y el puerto	Escritura	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateUserSettings [solo permiso]	Otorga permiso para actualizar la configuración específica del IDE de un usuario de Cloud9 AWS	Escritura			

Tipos de recursos definidos por AWS Cloud9

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment	`arn:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Cloud9

AWS Cloud9 define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
cloud9:EnvironmentId	Filtra el acceso por el ID del AWS entorno Cloud9	Cadena
cloud9:EnvironmentName	Filtra el acceso por el nombre del AWS entorno Cloud9	Cadena
cloud9:InstanceType	Filtra el acceso por tipo de instancia de la instancia Amazon del entorno AWS Cloud9 EC2	Cadena
cloud9:OwnerArn	Filtra el acceso según el ARN de propietario especificado.	ARN
cloud9:Permissions	Filtra el acceso por tipo de permisos de AWS Cloud9	Cadena
cloud9:SubnetId	Filtra el acceso por el ID de subred en el que se creará el entorno AWS Cloud9	Cadena
cloud9:UserArn	Filtra el acceso por el ARN de usuario especificado	ARN

Acciones, recursos y claves de condición para AWS CloudFormation

AWS CloudFormation (prefijo de servicio:`cloudformation`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CloudFormation
- Tipos de recursos definidos por AWS CloudFormation
- Claves de condición de AWS CloudFormation

Acciones definidas por AWS CloudFormation

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateOrganizationsAccess	Otorga permiso para activar el acceso confiable entre StackSets and Organizations. Con Trusted Access Between StackSets and Organizations activado, la cuenta de administración tiene permisos de creación y administración StackSets para su organización	Escritura			
ActivateType	Concede permiso para activar una extensión pública de terceros, lo que la pone a	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	disposición para su uso en plantillas de pila				
BatchDescribeTypeConfigurations	Otorga permiso para devolver los datos de configuración de las CloudFormation extensiones especificadas	Lectura			
CancelUpdateStack	Concede permiso para cancelar una actualización en la pila especificada.	Write	stack*		
ContinueUpdateRollback	Concede permiso para continuar restaurando una pila que se encuentra en estado UPDATE_ROLLBACK_FAILED al estado UPDATE_ROLLBACK_COMPLETE.	Write	stack*		
				cloudformation:RoleArn	
CreateChangeSet	Concede permiso para crear una lista de cambios para una pila.	Escritura	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				cloudformation:ChangeSetName cloudformation:ResourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateGeneratedTemplate	Otorga permiso para crear una plantilla a partir de los recursos existentes que aún no se administran CloudFormation	Escritura			
CreateStack	Concede permiso para crear una pila según se especifica en la plantilla.	Write	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateStackInstances	Concede permiso para crear instancias de pila para las cuentas especificadas, dentro de las regiones especificadas.	Escritura	stackset*		
			stackset-target		
			type		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys cloudformation:TargetRegion	
CreateStackRefactor	Otorga permiso para crear una refactorización de pila	Escritura	stack*		
CreateStackSet	Concede permiso para crear un conjunto de pila como se especifica en la plantilla.	Write		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateUploadBucket [solo permiso]	Concede permiso para cargar plantillas a los buckets de Simple Storage Service (Amazon S3). Solo lo usa la AWS CloudFormation consola y no está documentado en la referencia de la API	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeactivateOrganizationsAccess	Otorga permiso para desactivar el acceso confiable entre StackSets and Organizations. Si el acceso de confianza está desactivado, la cuenta de administración no tiene permisos para crear y administrar los servicios gestionados para su organización StackSets	Escritura			
DeactivateType	Concede permiso para desactivar una extensión pública que se había activado anteriormente en esta cuenta y región	Escritura			
DeleteChangeSet	Concede permiso para eliminar el conjunto de cambios especificado. Eliminar conjuntos de cambios garantiza que nadie ejecutará el conjunto de cambios equivocado.	Escritura	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	Concede permiso para eliminar una plantilla generada	Escritura			
DeleteStack	Concede permiso para eliminar una pila específica.	Write	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				cloudformation:RoleArn	
DeleteStackInstances	Concede permiso para eliminar instancias de pila para las cuentas especificadas, en las regiones especificadas.	Write	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
DeleteStackSet	Concede permiso para eliminar un conjunto de pilas específico.	Escritura	stackset*		
DeregisterType	Otorga permiso para anular el registro de un tipo o versión de tipo existente CloudFormation	Escritura			
DescribeAccountLimits	Otorga permiso para recuperar los límites de tu cuenta AWS CloudFormation	Lectura			
DescribeChangeSet	Concede permiso para devolver la descripción del conjunto de cambios especificado.	Lectura	stack*		
				cloudformation:ChangeSetName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeChangeSetHooks	Concede permiso para devolver la información de invocación de Hook para el conjunto de cambios especificado	Lectura	stack*		
				cloudformation:ChangeSetName	
DescribeGeneratedTemplate	Concede permiso para describir una plantilla generada. La salida incluye detalles sobre el avance en la creación de una plantilla generada	Lectura			
DescribeOrganizationsAccess	Otorga permiso para devolver información sobre el OrganizationAccess estado de la cuenta	Lectura			
DescribePublisher	Otorga permiso para devolver información sobre el editor CloudFormation de una extensión	Lectura			
DescribeResourceScan	Concede permiso para describir detalles de un análisis de recursos	Lectura			
DescribeStackDriftDetectionStatus	Concede permiso para devolver información sobre una operación de detección de desviación de pila.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeStackEvents	Concede permiso para devolver todos los eventos relacionados con la pila de una pila especificada.	Lectura	stack*		
DescribeStackInstance	Otorga permiso para devolver la instancia de pila que está asociada al conjunto de pilas y la región especificados Cuenta de AWS	Lectura	stackset*		
DescribeStackRefactor	Otorga permiso para devolver la descripción de la refactorización de pila especificada	Lectura	stack*		
DescribeStackResource	Concede permiso para devolver una descripción del recurso especificado en la pila especificada.	Read	stack*		
DescribeStackResourceDrifts	Concede permiso para devolver información de desviaciones de los recursos en los que se han comprobado las desviaciones en la pila especificada.	Lectura	stack*		
DescribeStackResources	Otorga permiso para devolver las descripciones AWS de los recursos de las pilas en ejecución y eliminadas	Lectura	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeStackSet	Concede permiso para devolver la descripción del conjunto de pilas especificado.	Read	stackset*		
DescribeStackSetOperation	Concede permiso para devolver la descripción de la operación de conjunto de pilas especificada.	Lectura	stackset*		
DescribeStacks	Otorga permiso para devolver la descripción de la pila especificada y de todas las pilas cuando se utilizan en combinación con la acción ListStacks	Enumeración	stack		cloudformation:ListStacks
DescribeType	Otorga permiso para devolver información sobre el CloudFormation tipo solicitado	Lectura			
DescribeTypeRegistration	Otorga permiso para devolver información sobre el proceso de registro de un CloudFormation tipo	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetectStackDrift	Concede permiso para detectar si la configuración real de una pila es diferente o se ha desviado de su configuración prevista, tal y como se define en la plantilla de pila y los valores especificados como parámetros de la plantilla.	Read	stack*		
DetectStackResourceDrift	Concede permiso para devolver información sobre si la configuración real de un recurso es diferente o se ha desviado de su configuración prevista, tal y como se define en la plantilla de pila y los valores especificados como parámetros de la plantilla.	Read	stack*		
DetectStackSetDrift	Concede permiso para permitir a los usuarios detectar la deriva en un conjunto de pila y las instancias de pila que pertenecen a ese conjunto de pila.	Read	stackset*		
EstimateTemplateCost	Concede permiso para devolver el costo mensual estimado de una plantilla.	Read		cloudformation:TemplateUrl	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExecuteChangeSet	Concede permiso para actualizar una pila con la información de entrada que se proporcionó cuando se creó el conjunto de cambios especificado.	Escritura	stack*		
				cloudformation:ChangeSetName	
ExecuteStackRefactor	Otorga permiso para ejecutar una refactorización de pila utilizando la información de entrada que se proporcionó al crear la refactorización de pila especificada	Escritura	stack*		
GetGeneratedTemplate	Concede permiso para recuperar una plantilla generada	Lectura			
GetStackPolicy	Concede permiso para devolver la política de pila para una pila especificada.	Read	stack*		
GetTemplate	Concede permiso para devolver el cuerpo de la plantilla para una pila especificada.	Read	stack*		
GetTemplateSummary	Concede permiso para devolver información sobre una plantilla nueva o existente.	Lectura	stack		
			stackset		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				cloudformation:TemplateUrl	
ImportStacksToStackSet	Concede permiso para permitir a los usuarios importar pilas existentes a un conjunto de pilas nuevo o existente	Escritura	stackset*		
ListChangeSets	Concede permiso para devolver el ID y el estado de cada conjunto de cambios activo de una pila. Por ejemplo, AWS CloudFormation enumera los conjuntos de cambios que se encuentran en el estado CREATE_IN_PROGRESS o CREATE_PENDING	Enumeración	stack*		
ListExports	Concede permiso para enumerar todos los valores de salida exportados en la cuenta y la región en la que se llama a esta acción.	Enumeración			
ListGeneratedTemplates	Concede permiso para enumerar las plantillas generadas en esta región	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListHookResults	Otorga permiso para devolver la información de los resultados de las invocaciones de Hook para el objetivo especificado	Enumeración	stack		
				cloudformation:ChangeSetName	
ListImports	Concede permiso para enumerar todas las pilas que importan un valor de salida exportado.	Enumeración			
ListResourceScanRelatedResources	Concede permiso para enumerar los recursos relacionados para una lista de recursos a partir de un análisis de recursos. La respuesta indica si cada recurso devuelto ya está gestionado por CloudFormation	Enumeración			
ListResourceScanResources	Concede permiso para enumerar los recursos de un análisis de recursos. Los resultados se pueden filtrar por identificador de recurso, prefijo de tipo de recurso, clave de etiqueta y valor de etiqueta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourceScans	Concede permiso para enumerar los análisis de recursos del más reciente al más antiguo. De forma predeterminada, devolverá hasta 10 análisis de recursos	Enumeración			
ListStackInstanceResourceDrifts	Concede permiso para devolver información de desviaciones de los recursos en los que se han comprobado las desviaciones en la instancia de la pila especificada	Enumeración	stackset*		
ListStackInstances	Concede permiso para devolver información resumida sobre instancias de pila asociadas al conjunto de pilas especificado.	Enumeración	stackset*		
ListStackRefactorActions	Otorga permiso para devolver la lista de acciones de la refactorización de pila especificada	Enumeración	stack*		
ListStackRefactors	Otorga permiso para devolver el ID y el estado de cada refactorización de pila activa	Enumeración	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStackResources	Concede permiso para devolver descripciones de todos los recursos de la pila especificada.	Enumeración	stack*		
ListStackSetAutoDeploymentTargets	Otorga permiso para devolver información resumida sobre los objetivos StackSet de despliegue automático	Enumeración	stackset*		
ListStackSetOperationResults	Concede permiso para devolver información resumida sobre los resultados de una operación de conjunto de pilas.	List	stackset*		
ListStackSetOperations	Concede permiso para devolver información resumida sobre operaciones realizadas en un conjunto de pilas.	List	stackset*		
ListStackSets	Concede permiso para devolver información resumida sobre conjuntos de pilas asociados con el usuario.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStacks	Otorga permiso para devolver la información resumida de las pilas cuyo estado coincida con el especificado StackStatusFilter. En combinación con la DescribeStacks acción, otorga permiso para enumerar las descripciones de las pilas	Enumeración			
ListTypeRegistrations	Otorga permiso para enumerar los intentos CloudFormation de registro del tipo	Enumeración			
ListTypeVersions	Otorga permiso para publicar versiones de un CloudFormation tipo concreto	Enumeración			
ListTypes	Otorga permiso para enumerar los CloudFormation tipos disponibles	Enumeración			
PublishType	Otorga permiso para publicar la extensión especificada en el CloudFormation registro como extensión pública en esta región	Escritura			
RecordHandlerProgress	Concede permiso para registrar el progreso del controlador	Escritura	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterPublisher	Otorga permiso para registrar una cuenta como publicadora de extensiones públicas en el CloudFormation registro	Escritura			
RegisterType	Otorga permiso para registrar un nuevo CloudFormation tipo	Escritura			
RollbackStack	Concede permiso para revertir la pila al último estado estable	Escritura	stack*		
				cloudformation:RoleArn	
SetStackPolicy	Concede permiso para establecer una política de pila para una pila especificada.	Administración de permisos	stack*		
				cloudformation:StackPolicyUrl	
SetTypeConfiguration	Otorga permiso para establecer los datos de configuración de una CloudFormation extensión registrada en la cuenta y la región en cuestión	Escritura			
SetTypeDefaultVersion	Otorga permiso para establecer qué versión de un CloudFormation tipo se aplica a CloudFormation las operaciones	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SignalResource	Concede permiso para enviar una señal al recurso especificado con un estado de éxito o error.	Escritura	stack*		
StartResourceScan	Concede permiso para iniciar un análisis de los recursos de esta cuenta en esta región	Escritura			
StopStackSetOperation	Concede permiso para detener una operación en curso en un conjunto de pilas y sus instancias de pila asociadas.	Write	stackset*		
TagResource	Concede permiso para etiquetar recursos de CloudFormation.	Etiquetado	changeset		
			stack		
			stackset		
				aws:TagKeys aws:RequestTag/${TagKey} cloudformation:CreateAction	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TestType	Otorga permiso para probar una extensión registrada para asegurarse de que cumple todos los requisitos necesarios para su publicación en el CloudFormation registro	Escritura			
UntagResource	Concede permiso para desetiquetar recursos de CloudFormation.	Etiquetado	changeset		
			stack		
			stackset		
				aws:TagKeys cloudformation:CreateAction	
UpdateGeneratedTemplate	Concede permiso para actualizar una plantilla generada. Esto se puede usar para cambiar el nombre, agregar y eliminar recursos, actualizar los recursos y cambiar la UpdateReplacePolicy configuración DeletionPolicy y	Escritura			
UpdateStack	Concede permiso para actualizar una pila según se especifica en la plantilla.	Write	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	Concede permiso para actualizar los valores de parámetros de las instancias de pila de las cuentas especificadas, dentro de las regiones especificadas.	Write	stackset*		
			stackset-target		
			type		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				cloudformation:TargetRegion	
UpdateStackSet	Concede permiso para actualizar un conjunto de pila según se especifica en la plantilla.	Write	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTerminationProtection	Concede permiso para actualizar la protección de terminación para la pila especificada.	Write	stack*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ValidateTemplate	Concede permiso para validar una plantilla especificada.	Lectura		cloudformation:TemplateUrl	

Tipos de recursos definidos por AWS CloudFormation

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

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

Tipos de recurso	ARN	Claves de condición
type	arn:${Partition}:cloudformation:${Region}:${Account}:type/resource/${Type}	
generated template	arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}	
resources can	arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}	

Claves de condición de AWS CloudFormation

AWS CloudFormation define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
cloudformation:ChangeSetName	Filtra el acceso por el nombre del conjunto de AWS CloudFormation cambios. Se utiliza para controlar qué conjuntos de cambios pueden ejecutar o eliminar los usuarios de IAM.	Cadena
cloudformation:CreateAction	Filtra el acceso por el nombre de una acción de API que muta un recurso. Se utiliza para controlar qué etiquetas pueden utilizar los usuarios de APIs IAM para añadir o eliminar etiquetas en una pila o conjunto de pilas	Cadena
cloudformation:ImportResourceTypes	Filtra el acceso por los tipos de recursos de la plantilla, como AWS:EC2: :Instance. Se utiliza para controlar con qué tipos de recursos pueden trabajar los usuarios de IAM cuando desean importar un recurso a una pila.	Cadena
cloudformation:ResourceTypes	Filtra el acceso por los tipos de recursos de la plantilla, como AWS:EC2: :Instance. Se utiliza para controlar con qué tipo de recursos pueden trabajar los usuarios de IAM al crear o actualizar una pila.	ArrayOfString
cloudformation:RoleArn	Filtra el acceso en función del ARN de una función de servicio de IAM. Se utiliza para controlar qué rol de servicio pueden utilizar los usuarios de IAM para trabajar con conjuntos de cambios o pilas.	ARN
cloudformation:StackPolicyUrl	Filtra el acceso en función de una URL de política de pila de Amazon S3. Se utiliza para controlar qué políticas de pila pueden asociar los usuarios de IAM a una pila durante una acción de creación o actualización de la pila.	Cadena
cloudformation:TargetRegion	Filtra el acceso por región de destino del conjunto de pila. Se utiliza para controlar qué regiones pueden usar los usuarios de IAM cuando crean o actualizan los conjuntos de pilas.	ArrayOfString

Claves de condición	Descripción	Tipo
cloudformation:TemplateUrl	Filtra el acceso en función de una URL de plantilla de Amazon S3. Se utiliza para controlar qué plantillas pueden usar los usuarios de IAM cuando crean o actualizan pilas.	Cadena

Acciones, recursos y claves de condición de Amazon CloudFront

Amazon CloudFront (prefijo de servicio:`cloudfront`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudFront
- Tipos de recursos definidos por Amazon CloudFront
- Claves de estado de Amazon CloudFront

Acciones definidas por Amazon CloudFront

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Otorga permiso para configurar la entrega vendida de registros para una distribución	Administración de permisos	distribution		
AssociateAlias	Otorga permiso para asociar un alias a una distribución CloudFront	Escritura	distribution*		
AssociateDistributionTenantWebACL	Otorga permiso para asociar un inquilino de distribución a una ACL web AWS de WAF	Escritura	distribution-tenant*		
AssociateDistributionWebACL	Otorga permiso para asociar una distribución a una ACL web de AWS WAF	Escritura	distribution*		
CopyDistribution	Otorga permiso para copiar una distribución existente y crear una nueva distribución web	Escritura	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAnycastIpList	Otorga permiso para crear una lista de IP estáticas de Anycast	Escritura	anycast-ip-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	Otorga permiso para añadir una nueva política de caché a CloudFront	Escritura	cache-policy*		
CreateCloudFrontOriginAccessIdentity	Otorga permiso para crear una nueva identidad de acceso al CloudFront origen	Escritura	origin-access-identity*		
CreateConnectionGroup	Otorga permiso para crear un grupo de conexiones	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContinuousDeploymentPolicy	Otorga permiso para añadir una nueva política de despliegue continuo a CloudFront	Escritura	continuous-deployment-policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDistribution	Concede permiso para crear una nueva distribución web	Escritura	distribution*		cloudfront:CreateConnectionGroup
CreateDistributionTenant	Otorga permiso para crear un inquilino de distribución	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFieldLevelEncryptionConfig	Concede permiso para crear una nueva configuración de cifrado en el nivel de campo	Write			
CreateFieldLevelEncryptionProfile	Concede permiso para crear un perfil de cifrado en el nivel de campo	Escritura			
CreateFunction	Otorga permiso para crear una CloudFront función	Escritura	function*		
CreateInvalidation	Concede permiso para crear una nueva solicitud de lote de invalidación	Escritura	distribution*		
CreateInvalidationForDistributionTenant	Otorga permiso para crear una invalidación para un arrendatario de distribución	Escritura	distribution-tenant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateKeyGroup	Otorga permiso para añadir un nuevo grupo de claves a CloudFront	Escritura			
CreateKeyValueStore	Otorga permiso para crear un CloudFront KeyValueStore	Escritura	key-value-store*		
CreateMonitoringSubscription	Otorga permiso para habilitar CloudWatch métricas adicionales para la CloudFront distribución especificada. Las métricas adicionales incurren en un costo adicional	Escritura			
CreateOriginAccessControl	Concede permiso para crear un nuevo control de acceso de origen	Escritura			
CreateOriginRequestPolicy	Otorga permiso para añadir una nueva política de solicitudes de origen a CloudFront	Escritura	origin-request-policy*		
CreatePublicKey	Otorga permiso para añadir una nueva clave pública a CloudFront	Escritura			
CreateRealtimeLogConfig	Concede permiso para crear una configuración de registro en tiempo real	Escritura	realtime-log-config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateResponseHeadersPolicy	Otorga permiso para añadir una nueva política de encabezados de respuesta a CloudFront	Escritura	response-headers-policy*		
CreateSavingsPlan [solo permiso]	Concede permiso para crear un nuevo Savings Plan	Escritura			
CreateStreamingDistribution	Concede permiso para crear una nueva distribución RTMP	Write	streaming-distribution*		
CreateStreamingDistributionWithTags	Concede permiso para crear una nueva distribución RTMP con etiquetas	Escritura	streaming-distribution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcOrigin	Concede permiso para crear un origen de VPC	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAnycastIpList	Otorga permiso para eliminar una lista de IP estáticas de Anycast	Escritura	anycast-ip-list*		
DeleteCachePolicy	Concede permiso para eliminar una política de caché	Escritura	cache-policy*		
DeleteCloudFrontOriginAccessIdentity	Otorga permiso para eliminar una identidad de acceso de CloudFront origen	Escritura	origin-access-identity*		
DeleteConnectionGroup	Otorga permiso para eliminar un grupo de conexiones	Escritura	connection-group*		
DeleteContinuousDeploymentPolicy	Otorga permiso para eliminar una política de implementación continua	Escritura	continuous-deployment-policy*		
DeleteDistribution	Concede permiso para eliminar una distribución web	Escritura	distribution*		
DeleteDistributionTenant	Otorga permiso para eliminar un inquilino de distribución	Escritura	distribution-tenant*		
DeleteFieldLevelEncryptionConfig	Concede permiso para eliminar una configuración de cifrado en el nivel de campo	Write	field-level-encryption-config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFieldLevelEncryptionProfile	Concede permiso para eliminar un perfil de cifrado en el nivel de campo	Escritura	field-level-encryption-profile*		
DeleteFunction	Otorga permiso para eliminar una CloudFront función	Escritura	function*		
DeleteKeyGroup	Concede permiso para eliminar un grupo de claves	Escritura			
DeleteKeyValueStore	Otorga permiso para eliminar una CloudFront KeyValueStore	Escritura	key-value-store*		
DeleteMonitoringSubscription	Otorga permiso para deshabilitar CloudWatch métricas adicionales para la CloudFront distribución especificada	Escritura			
DeleteOriginAccessControl	Concede permiso para eliminar un control de acceso de origen	Escritura	origin-access-control*		
DeleteOriginRequestPolicy	Concede permiso para eliminar una política de solicitud de origen	Escritura	origin-request-policy*		
DeletePublicKey	Otorga permiso para eliminar una clave pública de CloudFront	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRealtimeLogConfig	Concede permiso para eliminar una configuración de registro en tiempo real	Escritura	realtime-log-config*		
DeleteResponseHeadersPolicy	Concede permiso para eliminar una política de encabezados de respuesta.	Escritura	response-headers-policy*		
DeleteStreamingDistribution	Concede permiso para eliminar una distribución RTMP	Escritura	streaming-distribution*		
DeleteVpcOrigin	Concede permiso para eliminar un origen de VPC	Escritura	vpcorigin*		
DescribeFunction	Otorga permiso para obtener un resumen de CloudFront la función	Lectura	function*		
DescribeKeyValueStore	Otorga permiso para obtener un CloudFront KeyValueStore resumen	Lectura	key-value-store*		
DisassociateDistributionTenantWebACL	Otorga permiso para desasociar un inquilino de distribución de una ACL web de AWS WAF	Escritura	distribution-tenant*		
DisassociateDistributionWebACL	Otorga permiso para desasociar una distribución de una ACL web de WAF AWS	Escritura	distribution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAnycastIpList	Otorga permiso para obtener una lista de IP estáticas de Anycast	Lectura	anycast-ip-list*		
GetCachePolicy	Concede permiso para obtener la política de caché	Read	cache-policy*		
GetCachePolicyConfig	Concede permiso para obtener la configuración de la política de caché	Lectura	cache-policy*		
GetCloudFrontOriginAccessIdentity	Otorga permiso para obtener la información sobre una identidad de acceso de CloudFront origen	Lectura	origin-access-identity*		
GetCloudFrontOriginAccessIdentityConfig	Concede permiso para obtener información de configuración sobre una identidad de acceso de origen de CloudFront	Lectura	origin-access-identity*		
GetConnectionGroup	Otorga permiso para obtener información sobre un grupo de conexión	Lectura	connection-group*		
GetConnectionGroupByRoutingEndpoint	Otorga permiso para obtener información sobre un grupo de conexiones mediante el extremo de enrutamiento especificado	Lectura	connection-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetContinuousDeploymentPolicy	Otorga permiso para obtener la política de implementación continua	Lectura	continuous-deployment-policy*		
GetContinuousDeploymentPolicyConfig	Otorga permiso para obtener la configuración de la política de implementación continua	Lectura	continuous-deployment-policy*		
GetDistribution	Concede permiso para obtener información acerca de la distribución web	Read	distribution*		
GetDistributionConfig	Concede permiso para obtener información de configuración acerca de una distribución	Lectura	distribution*		
GetDistributionTenant	Otorga permiso para obtener información sobre un arrendatario de distribución	Lectura	distribution-tenant*		
GetDistributionTenantByDomain	Otorga permiso para obtener información sobre un arrendatario de distribución por el dominio asociado	Lectura	distribution-tenant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFieldLevelEncryption	Concede permiso para obtener la información de configuración de cifrado en el nivel de campo	Read	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	Concede permiso para obtener la información de configuración de cifrado en el nivel de campo	Read	field-level-encryption-config*		
GetFieldLevelEncryptionProfile	Concede permiso para obtener la información de configuración de cifrado en el nivel de campo	Read	field-level-encryption-profile*		
GetFieldLevelEncryptionProfileConfig	Concede permiso para obtener la información de configuración del perfil de cifrado en el nivel de campo	Lectura	field-level-encryption-profile*		
GetFunction	Otorga permiso para obtener el código de una CloudFront función	Lectura	function*		
GetInvalidation	Concede permiso para obtener información sobre una invalidación	Lectura	distribution*		
GetInvalidationForDistributionTenant	Otorga permiso a un arrendatario de distribución para obtener información sobre una invalidación	Lectura	distribution-tenant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetKeyGroup	Concede permiso para obtener un grupo de claves	Read			
GetKeyGroupConfig	Concede permiso para obtener una configuración de grupo de claves	Lectura			
GetManagedCertificateDetails	Otorga permiso para obtener detalles sobre un certificado CloudFront gestionado	Lectura	distribution-tenant*		
GetMonitoringSubscription	Otorga permiso para obtener información sobre si están habilitadas CloudWatch métricas adicionales para la CloudFront distribución especificada	Lectura			
GetOriginAccessControl	Concede permiso para obtener el control de acceso de origen	Lectura	origin-access-control*		
GetOriginAccessControlConfig	Concede permiso para obtener la configuración del control de acceso de origen	Lectura	origin-access-control*		
GetOriginRequestPolicy	Concede permiso para obtener la política de solicitud de origen	Read	origin-request-policy*		
GetOriginRequestPolicyConfig	Concede permiso para obtener la configuración de la política de solicitud de origen	Read	origin-request-policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPublicKey	Concede permiso para obtener la información de clave pública	Read			
GetPublicKeyConfig	Concede permiso para obtener la información de la configuración de clave pública	Read			
GetRealtimeLogConfig	Concede permiso para obtener una configuración de registro en tiempo real	Lectura	realtime-log-config*		
GetResponseHeadersPolicy	Concede permiso para obtener la política de encabezados de respuesta.	Lectura	response-headers-policy*		
GetResponseHeadersPolicyConfig	Concede permiso para obtener la configuración de la política de encabezados de respuesta.	Lectura	response-headers-policy*		
GetSavingsPlan [solo permiso]	Concede permiso para obtener un Savings Plan	Lectura			
GetStreamingDistribution	Concede permiso para obtener información acerca de la distribución RTMP	Read	streaming-distribution*		
GetStreamingDistributionConfig	Concede permiso para obtener información de configuración acerca de una distribución de streaming	Lectura	streaming-distribution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVpcOrigin	Otorga permiso para obtener la información sobre el origen de una VPC	Lectura	vpcorigin*		
ListAnycastIpLists	Otorga permiso para incluir sus listas de IP estáticas de Anycast	Enumeración			
ListCachePolicies	Otorga permiso para enumerar todas las políticas de caché que se han creado CloudFront para esta cuenta	Enumeración			
ListCloudFrontOriginAccessIdentities	Otorga permiso para enumerar tus identidades de acceso a CloudFront origen	Enumeración			
ListConflictingAliases	Otorga permiso para enumerar todos los alias que entran en conflicto con el alias indicado en CloudFront	Enumeración	distribution*		
ListConnectionGroups	Otorga permiso para enumerar los grupos de conexiones de su Cuenta de AWS	Enumeración			
ListContinuousDeploymentPolicies	Otorga permiso para enumerar todas las políticas de implementación continua de la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDistributionTenants	Otorga permiso para incluir los inquilinos de distribución de su Cuenta de AWS	Enumeración			
ListDistributionTenantsByCustomization	Otorga permiso para enumerar los inquilinos de la distribución según la personalización que especifique	Enumeración			
ListDistributions	Otorga permiso para enumerar las distribuciones asociadas a su Cuenta de AWS	Enumeración			
ListDistributionsByAnycastIpListId	Otorga permiso para incluir en su cuenta las distribuciones asociadas a la especificada AnycastIpListId	Enumeración			
ListDistributionsByCachePolicyId	Otorga permiso IDs para incluir en la lista la distribución de las distribuciones que tienen un comportamiento de caché asociado a la política de caché especificada	Enumeración			
ListDistributionsByConnectionMode	Otorga permiso para enumerar las distribuciones según el modo de conexión especificado	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDistributionsByKeyGroup	Otorga permiso IDs para enumerar la distribución de las distribuciones que tienen un comportamiento de caché asociado al grupo de claves especificado	Enumeración			
ListDistributionsByLambdaFunction [solo permiso]	Concede permiso para enumerar las distribuciones asociadas a la función de Lambda	Enumeración			
ListDistributionsByOriginRequestPolicyId	Otorga permiso IDs para publicar la distribución de las distribuciones que tienen un comportamiento de caché asociado a la política de solicitudes de origen especificada	Enumeración			
ListDistributionsByRealtimeLogConfig	Concede permiso para obtener una lista de distribuciones que tienen un comportamiento de memoria en caché asociado a la configuración de registro en tiempo real especificada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDistributionsByResponseHeadersPolicyId	Otorga permiso IDs para publicar la distribución de las distribuciones que tienen un comportamiento de caché asociado a la política de encabezados de respuesta especificada	Enumeración			
ListDistributionsByVpcOriginId	Otorga permiso IDs para publicar distribuciones asociadas al origen de VPC especificado	Enumeración			
ListDistributionsByWebACLId	Otorga permiso para publicar las distribuciones asociadas a su ACL web de Cuenta de AWS WAF determinada AWS	Enumeración			
ListDomainConflicts	Otorga permiso para enumerar los conflictos de dominio de un dominio específico	Enumeración	distribution		
			distribution-tenant		
ListFieldLevelEncryptionConfigs	Otorga permiso para enumerar todas las configuraciones de cifrado a nivel de campo que se han creado CloudFront para esta cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFieldLevelEncryptionProfiles	Otorga permiso para enumerar todos los perfiles de cifrado a nivel de campo que se han creado para esta cuenta CloudFront	Enumeración			
ListFunctions	Otorga permiso para obtener una lista de funciones CloudFront	Enumeración			
ListInvalidations	Concede permiso para enumerar los lotes de invalidación	Enumeración	distribution*		
ListInvalidationsForDistributionTenant	Otorga permiso para enumerar las invalidaciones de un arrendatario de distribución	Enumeración	distribution-tenant*		
ListKeyGroups	Otorga permiso para enumerar todos los grupos clave que se han creado CloudFront para esta cuenta	Enumeración			
ListKeyValueStores	Otorga permiso para obtener una lista de CloudFront KeyValueStores	Enumeración			
ListOriginAccessControls	Concede permiso para enumerar todos los controles de acceso de origen de la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOriginRequestPolicies	Otorga permiso para enumerar todas las políticas de solicitudes de origen que se han creado CloudFront para esta cuenta	Enumeración			
ListPublicKeys	Otorga permiso para enumerar todas las claves públicas que se han agregado CloudFront a esta cuenta	Enumeración			
ListRateCards [solo permiso]	Otorga permiso para incluir las tarjetas CloudFront de tarifas de la cuenta	Enumeración			
ListRealtimeLogConfigs	Concede permiso para obtener una lista de configuraciones de registro en tiempo real	Enumeración			
ListResponseHeadersPolicies	Otorga permiso para enumerar todas las políticas de encabezados de respuesta que se han creado CloudFront para esta cuenta	Enumeración			
ListSavingsPlans [solo permiso]	Concede permiso para enumerar los Savings Plans de la cuenta	Enumeración			
ListStreamingDistributions	Concede permiso para enumerar sus distribuciones RTMP	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso CloudFront	Lectura	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		
			vpcorigin		
ListUsages [solo permiso]	Otorga permiso para enumerar CloudFront el uso	Enumeración			
ListVpcOrigins	Otorga permiso para enumerar los orígenes de la VPC	Enumeración			
PublishFunction	Otorga permiso para publicar una función CloudFront	Escritura	function*		
TagResource	Otorga permiso para añadir etiquetas a un CloudFront recurso	Etiquetado	anycast-ip-list		
			connection-group		
			distribution		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			distribution-tenant		
			streaming-distribution		
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestFunction	Otorga permiso para probar una CloudFront función	Escritura	function*		
UntagResource	Otorga permiso para eliminar etiquetas de un CloudFront recurso	Etiquetado	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			streaming-distribution		
			vpcorigin		
				aws:TagKeys	
UpdateCachePolicy	Concede permiso para actualizar una política de caché	Escritura	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	Otorga permiso para establecer la configuración de una identidad de acceso de CloudFront origen	Escritura	origin-access-identity*		
UpdateConnectionGroup	Otorga permiso para actualizar un grupo de conexiones	Escritura	connection-group*		
UpdateContinuousDeploymentPolicy	Otorga permiso para actualizar una política de implementación continua	Escritura	continuous-deployment-policy*		
UpdateDistribution	Concede permiso para actualizar la configuración de una distribución web	Escritura	distribution*		
UpdateDistributionTenant	Otorga permiso para actualizar un inquilino de distribución	Escritura	distribution-tenant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDistributionWithStagingConfig	Concede permiso para copiar la configuración de una distribución web de ensayo a su correspondiente distribución web principal	Escritura	distribution*		
UpdateDomainAssociation	Otorga permiso para actualizar una asociación de dominios	Escritura	distribution		
			distribution-tenant		
UpdateFieldLevelEncryptionConfig	Concede permiso para actualizar la configuración de cifrado en el nivel de campo	Write			
UpdateFieldLevelEncryptionProfile	Concede permiso para actualizar un perfil de cifrado en el nivel de campo	Escritura	field-level-encryption-profile*		
UpdateFunction	Otorga permiso para actualizar una CloudFront función	Escritura	function*		
UpdateKeyGroup	Concede permiso para actualizar un grupo de claves	Escritura			
UpdateKeyValueStore	Otorga permiso para actualizar una CloudFront KeyValueStore	Escritura	key-value-store*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateOriginAccessControl	Concede permiso para actualizar un control de acceso de origen	Escritura	origin-access-control*		
UpdateOriginRequestPolicy	Concede permiso para actualizar una política de solicitud de origen	Write	origin-request-policy*		
UpdatePublicKey	Concede permiso para actualizar la información de clave pública	Write			
UpdateRealtimeLogConfig	Concede permiso para actualizar una configuración de registro en tiempo real	Escritura	realtime-log-config*		
UpdateResponseHeadersPolicy	Concede permiso para actualizar una política de encabezados de respuesta.	Escritura	response-headers-policy*		
UpdateSavingsPlan [solo permiso]	Concede permiso para actualizar un Savings Plan	Escritura			
UpdateStreamingDistribution	Concede permiso para actualizar la configuración de una distribución RTMP	Escritura	streaming-distribution*		
UpdateVpcOrigin	Concede permiso para actualizar el origen de una VPC	Escritura	vpcorigin*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
VerifyDnsConfiguration	Otorga permiso para verificar la configuración de DNS de un dominio específico	Lectura	distribution-tenant		

Tipos de recursos definidos por Amazon CloudFront

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
distribution	`arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}`	aws:ResourceTag/${TagKey}
streaming-distribution	`arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}`	aws:ResourceTag/${TagKey}
origin-access-identity	`arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}`	
field-level-encryption-config	`arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}`	

Tipos de recurso	ARN	Claves de condición
field-level-encryption-profile	arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}	
cache-policy	arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}	
origin-request-policy	arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}	
realtime-log-config	arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}	
function	arn:${Partition}:cloudfront::${Account}:function/${Name}	
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	
continuous-deployment-policy	arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}	
anycast-ip-list	arn:${Partition}:cloudfront::${Account}:anycast-ip-list/${Id}	aws:ResourceTag/${TagKey}
vpcorigin	arn:${Partition}:cloudfront::${Account}:vpcorigin/${Id}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
distribution-tenant	arn:${Partition}:cloudfront::${Account}:distribution-tenant/${Id}	aws:ResourceTag/${TagKey}
connection-group	arn:${Partition}:cloudfront::${Account}:connection-group/${Id}	aws:ResourceTag/${TagKey}

Claves de estado de Amazon CloudFront

Amazon CloudFront define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon CloudFront KeyValueStore

Amazon CloudFront KeyValueStore (prefijo de servicio:`cloudfront-keyvaluestore`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudFront KeyValueStore
- Tipos de recursos definidos por Amazon CloudFront KeyValueStore
- Claves de estado de Amazon CloudFront KeyValueStore

Acciones definidas por Amazon CloudFront KeyValueStore

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteKey	Concede permiso para eliminar el par clave-valor especificado por la clave	Escritura	key-value-store*		
DescribeKeyValueStore	Concede permiso para devolver información sobre los metadatos de un almacenamiento de clave-valor	Lectura	key-value-store*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetKey	Concede permiso para devolver un par clave-valor	Lectura	key-value-store*		
ListKeys	Concede permiso para devolver una lista de pares clave-valor	Enumeración	key-value-store*		
PutKey	Concede permiso para crear un nuevo par clave-valor o reemplazar el valor de una clave existente	Escritura	key-value-store*		
UpdateKeys	Otorga permiso para colocar o eliminar varios pares de valores clave en una sola operación all-or-nothing	Escritura	key-value-store*		

Tipos de recursos definidos por Amazon CloudFront KeyValueStore

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
key-value-store	`arn:${Partition}:cloudfront::${Account}:key-value-store/${ResourceId}`	

Claves de estado de Amazon CloudFront KeyValueStore

CloudFront KeyValueStore no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS CloudHSM

AWS CloudHSM (prefijo de servicio`cloudhsm`:) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CloudHSM
- Tipos de recursos definidos por AWS CloudHSM
- Claves de condición para AWS CloudHSM

Acciones definidas por AWS CloudHSM

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CopyBackupToRegion	Otorga permiso para crear una copia de seguridad en la región especificada	Escritura	backup*		cloudhsm:CopyBackupToRegion cloudhsm:TagResource cloudhsm:UntagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Concede permiso para crear un nuevo clúster de AWS CloudHSM	Escritura	backup		cloudhsm:TagResource ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateHsm	Concede permiso para crear un nuevo módulo de seguridad de hardware (HSM) en el clúster de AWS CloudHSM especificado	Escritura	cluster*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:RevokeSecurityGroupEgress
DeleteBackup	Otorga permiso para eliminar la copia de seguridad especificada	Escritura	backup*		
DeleteCluster	Concede permiso para eliminar el clúster de AWS CloudHSM especificado	Escritura	cluster*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup
DeleteHsm	Otorga permiso para eliminar el HSM especificado	Escritura			ec2:DeleteNetworkInterface
DeleteResourcePolicy	Concede permiso para eliminar la política asociada a los recursos de CloudHSM	Escritura	backup*		
DescribeBackups	Otorga permiso para obtener información sobre las copias de seguridad de los clústeres de AWS CloudHSM	Lectura			
DescribeClusters	Otorga permiso para obtener información sobre los clústeres de AWS CloudHSM	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourcePolicy	Otorga permiso para obtener información sobre la política adjunta a un recurso de AWS CloudHSM	Lectura	backup*		
InitializeCluster	Otorga permiso para reclamar un clúster de AWS CloudHSM	Escritura	cluster*		
ListTags	Otorga permiso para obtener una lista de etiquetas para el clúster de AWS CloudHSM especificado	Lectura	backup cluster		
ModifyBackupAttributes	Otorga permiso para modificar los atributos de una copia de seguridad de AWS CloudHSM	Escritura	backup*		
ModifyCluster	Concede permiso para modificar el clúster de AWS CloudHSM	Escritura	cluster*		ec2:DescribeSubnets
PutResourcePolicy	Otorga permiso para adjuntar una política a un recurso de AWS CloudHSM	Escritura	backup*		
RestoreBackup	Otorga permiso para restaurar la copia de seguridad de CloudHSM especificada	Escritura	backup*		
TagResource	Otorga permiso para añadir o sobrescribir una o más etiquetas para el clúster de AWS CloudHSM especificado	Etiquetado	backup cluster		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar la etiqueta o etiquetas especificadas del clúster de AWS CloudHSM especificado	Etiquetado	backup		
			cluster		
				aws:TagKeys	

Tipos de recursos definidos por AWS CloudHSM

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS CloudHSM

AWS CloudHSM define las siguientes claves de condición que se pueden usar en `Condition` el elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon CloudSearch

Amazon CloudSearch (prefijo de servicio:`cloudsearch`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudSearch
- Tipos de recursos definidos por Amazon CloudSearch
- Claves de estado de Amazon CloudSearch

Acciones definidas por Amazon CloudSearch

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTags	Adjunta etiquetas de recursos a un dominio de Amazon CloudSearch	Etiquetado	domain*		
BuildSuggesters	Indexa las sugerencias de búsqueda	Escritura	domain*		
CreateDomain	Crea un nuevo dominio de búsqueda	Escritura	domain*		
DefineAnalysisScheme	Configura un esquema de análisis que puede aplicarse a un campo de texto o de matriz de texto para definir las opciones de procesamiento de texto específicas de un idioma	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DefineExpression	Configura una expresión para el dominio de búsqueda	Escritura	domain*		
DefineIndexField	Configura un IndexField para el dominio de búsqueda	Escritura	domain*		
DefineSuggester	Configura un proveedor de sugerencias para un dominio	Escritura	domain*		
DeleteAnalysisScheme	Elimina un esquema de análisis	Escritura	domain*		
DeleteDomain	Elimina de forma permanente un dominio de búsqueda y todos sus datos	Escritura	domain*		
DeleteExpression	Quita una expresión del dominio de búsqueda	Escritura	domain*		
DeleteIndexField	Elimina an IndexField del dominio de búsqueda	Escritura	domain*		
DeleteSuggester	Elimina un proveedor de sugerencias	Escritura	domain*		
DescribeAnalysisSchemes	Obtiene los esquemas de análisis configurados para un dominio	Lectura	domain*		
DescribeAvailabilityOptions	Obtiene las opciones de disponibilidad configuradas para un dominio	Lectura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDomainEndpointOptions	Obtiene las opciones de punto de conexión de dominio configuradas para un dominio	Lectura	domain*		
DescribeDomains	Obtiene información sobre los dominios de búsqueda que son propiedad de esta cuenta	Enumeración	domain*		
DescribeExpressions	Obtiene las expresiones configuradas para el dominio de búsqueda	Lectura	domain*		
DescribeIndexFields	Obtiene información sobre los campos de índice configurados para el dominio de búsqueda	Lectura	domain*		
DescribeScalingParameters	Obtiene los parámetros de escalado configurados para un dominio	Lectura	domain*		
DescribeServiceAccessPolicies	Obtiene información sobre las políticas de acceso que controlan el acceso al documento y los puntos de conexión de búsqueda del dominio	Lectura	domain*		
DescribeSuggesters	Obtiene los proveedores de sugerencias configurados para un dominio	Lectura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
IndexDocuments	Indica al dominio de búsqueda que comience a indexar los documentos con las últimas opciones de indexación	Escritura	domain*		
ListDomainNames	Enumera todos los dominios de búsqueda propiedad de una cuenta	Enumeración	domain*		
ListTags	Muestra todas las etiquetas de recursos de un CloudSearch dominio de Amazon	Lectura	domain*		
RemoveTags	Quita las etiquetas de recursos especificadas de un dominio de Amazon ES	Etiquetado	domain*		
UpdateAvailabilityOptions	Configura las opciones de disponibilidad para un dominio	Escritura	domain*		
UpdateDomainEndpointOptions	Configura las opciones de punto de conexión de dominio para un dominio	Escritura	domain*		
UpdateScalingParameters	Configura los parámetros de escalado para un dominio	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceAccessPolicies	Configura las reglas de acceso que controlan el acceso al documento y los puntos de conexión de búsqueda del dominio	Administración de permisos	domain*		
document [solo permiso]	Permite el acceso a las operaciones de servicio de documentos	Escritura	domain		
search [solo permiso]	Permite el acceso a las operaciones de búsqueda	Lectura	domain		
suggest [solo permiso]	Permite el acceso a las operaciones de sugerencia	Lectura	domain		

Tipos de recursos definidos por Amazon CloudSearch

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> Para obtener información sobre el uso de CloudSearch los recursos de Amazon ARNs en una política de IAM, consulte Amazon CloudSearch ARNs en la Guía para CloudSearch desarrolladores de Amazon.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}`	

Claves de estado de Amazon CloudSearch

CloudSearch no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS CloudShell

AWS CloudShell (prefijo de servicio:`cloudshell`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CloudShell
- Tipos de recursos definidos por AWS CloudShell
- Claves de condición de AWS CloudShell

Acciones definidas por AWS CloudShell

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApproveCommand [solo permiso]	Otorga permiso para aprobar un comando enviado por otro servicio AWS	Lectura	Environment*		
CreateEnvironment [solo permiso]	Otorga permisos para crear un CloudShell entorno	Escritura		cloudshell:SecurityGroupIds cloudshell:SubnetIds cloudshell:VpcIds	
CreateSession [solo permiso]	Otorga permisos para conectarse a un CloudShell entorno desde AWS Management Console	Escritura	Environment*		
DeleteEnvironment [solo permiso]	Otorga permiso para eliminar un CloudShell entorno	Escritura	Environment*		
DescribeEnvironments [solo permiso]	Concede permiso para devolver descripciones de entornos de usuarios existentes	Enumeración			
GetEnvironmentStat	Otorga permiso para leer el estado de un CloudShell entorno	Lectura	Environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
us [solo permiso]					
GetFileDownloadUrls [solo permiso]	Otorga permisos para descargar archivos de un CloudShell entorno	Escritura	Environment*		
GetFileUploadUrls [solo permiso]	Otorga permisos para cargar archivos a un CloudShell entorno	Escritura	Environment*		
PutCredentials [solo permiso]	Concede permisos para reenviar credenciales de consola al entorno	Write	Environment*		
StartEnvironment [solo permiso]	Otorga permiso para iniciar un CloudShell entorno detenido	Escritura	Environment*		
StopEnvironment [solo permiso]	Otorga permiso para detener un CloudShell entorno en ejecución	Escritura	Environment*		

Tipos de recursos definidos por AWS CloudShell

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Environment	`arn:${Partition}:cloudshell:${Region}:${Account}:environment/${EnvironmentId}`	

Claves de condición de AWS CloudShell

AWS CloudShell define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
cloudshell:SecurityGroupIds	Filtra el acceso por ID de grupos de seguridad Disponible durante el CreateEnvironment funcionamiento	ArrayOfString
cloudshell:SubnetIds	Filtra el acceso según los ID de subred. Disponible durante el CreateEnvironment funcionamiento	ArrayOfString
cloudshell:VpcIds	Filtra el acceso según los ID de VPC. Disponible durante el CreateEnvironment funcionamiento	ArrayOfString

Acciones, recursos y claves de condición para AWS CloudTrail

AWS CloudTrail (prefijo de servicio:`cloudtrail`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CloudTrail
- Tipos de recursos definidos por AWS CloudTrail
- Claves de condición de AWS CloudTrail

Acciones definidas por AWS CloudTrail

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTags	Otorga permiso para añadir una o más etiquetas a una ruta, un almacén de datos de eventos, un canal o un panel de control, hasta un límite de 50	Etiquetado	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelQuery	Concede permiso para cancelar una consulta en ejecución	Escritura	eventdatastore*		
CreateChannel	Da permiso para crear un canal.	Escritura	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Otorga permiso para crear un panel	Escritura	dashboard*		cloudtrail:AddTags cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventDataStore	Concede permiso para crear un almacén de datos de eventos	Escritura	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceLinkedChannel [solo permiso]	Otorga permiso para crear un canal vinculado a un servicio que especifique la configuración para la entrega de datos de registro a un servicio AWS	Escritura	channel*		
CreateTrail	Da permiso para crear un registro de seguimiento que especifique la configuración de entrega de datos de registro a un bucket de Amazon S3.	Escritura	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Da permiso para eliminar un canal.	Escritura	channel*		
DeleteDashboard	Concede permiso para eliminar un panel	Escritura	dashboard*		
DeleteEventDataStore	Concede permiso para eliminar almacén de datos de eventos	Escritura	eventdatastore*		
DeleteResourcePolicy	Otorga permiso para eliminar la política de recursos de un recurso proporcionado	Escritura	channel		
			dashboard		
			eventdatastore		
DeleteServiceLinkedChannel [solo permiso]	Concede permiso para eliminar un canal vinculado a un servicio	Escritura	channel*		
DeleteTrail	Da permiso para eliminar un registro de seguimiento.	Escritura	trail*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterOrganizationDelegatedAdmin	Otorga permiso para anular el registro de una cuenta de miembro de AWS Organizations como administrador delegado	Escritura			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization
DescribeQuery	Concede permiso para enumerar los detalles de la consulta	Lectura	eventdatastore*		
DescribeTrails	Da permiso para enumerar la configuración de los registros de seguimiento asociados a la región actual de la cuenta.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableFederation	Otorga permiso para deshabilitar la federación de los datos del almacén de datos de eventos mediante el catálogo de datos de AWS Glue	Escritura	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableFederation	Otorga permiso para habilitar la federación de los datos del almacén de datos de eventos mediante el catálogo de datos de AWS Glue	Escritura	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	Otorga permiso para generar una consulta para un banco de datos de eventos específico mediante el generador de consultas CloudTrail Lake	Escritura	eventdatastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateQueryResultsSummary [solo permiso]	Otorga permiso para generar un resumen de resultados para consultas específicas mediante el generador de lenguaje CloudTrail natural	Lectura	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	Concede permiso para devolver información acerca de un canal específico	Lectura	channel*		
GetDashboard	Otorga permiso para enumerar la configuración del panel	Lectura	dashboard*		
GetEventConfiguration	Otorga permiso para enumerar las configuraciones de eventos que están configuradas para un banco de datos de eventos	Lectura	eventdatastore*		
GetEventDataStore	Concede permiso para enumerar las configuraciones para el almacén de datos de eventos	Lectura	eventdatastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEventDataStoreData	Otorga permiso para obtener datos de un banco de datos de eventos mediante el catálogo de datos de AWS Glue	Lectura	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetEventSelectors	Da permiso para obtener una lista de selectores de eventos configurados para un registro de seguimiento.	Lectura	trail*		
GetImport	Concede permiso para devolver información acerca de una importación específica	Lectura			
GetInsightSelectors	Otorga permiso para enumerar los selectores de CloudTrail Insights que están configurados para un banco de datos de senderos o eventos	Lectura	eventdatastore		
			trail		
GetQueryResults	Concede permiso para obtener los resultados de una consulta completa	Lectura	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy	Otorga permiso para obtener la política de recursos asociada al recurso proporcionado	Lectura	channel		
			dashboard		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			eventdatastore		
GetServiceLinkedChannel [solo permiso]	Concede permiso para enumerar los ajustes del canal vinculado a un servicio	Lectura	channel*		
GetTrail	Concede permiso para enumerar la configuración de la pista	Read	trail*		
GetTrailStatus	Da permiso para recuperar una lista con formato JSON de información sobre el registro de seguimiento especificado.	Lectura	trail*		
ListChannels	Concede permiso para enumerar los canales de la cuenta actual y sus nombres de origen	Enumeración			
ListDashboards	Otorga permiso para enumerar los paneles asociados a la región actual de su cuenta	Enumeración			
ListEventDataStores	Concede permiso para enumerar los almacenes de datos de eventos asociados a la región actual de la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListImportFailures	Concede permiso para devolver una lista de errores de la importación especificada	Lectura			
ListImports	Otorga permiso para devolver información sobre todas las importaciones o un conjunto selecto de importaciones por ImportStatus destino	Enumeración			
ListPublicKeys	Da permiso para obtener una lista de las claves públicas cuyas claves privadas se hayan utilizado para firmar los archivos de resumen de seguimiento dentro de un intervalo de tiempo especificado.	Lectura			
ListQueries	Concede permiso para enumerar las consultas asociadas con un almacén de datos de eventos	Enumeración	eventdatastore*		
ListServiceLinkedChannels [solo permiso]	Concede permiso para enumerar los canales vinculados a un servicio asociados a la región actual de una cuenta especificada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTags	Otorga permiso para incluir las etiquetas de las rutas, los almacenes de datos de eventos, los canales o los paneles de control de la región actual	Lectura	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	Da permiso para enumerar los registros de seguimiento asociados a la región actual de la cuenta.	Enumeración			
LookupEvents	Otorga permiso para buscar y recuperar datos métricos de los eventos de actividad de la API capturados por los CloudTrail que se crean, actualizan o eliminan recursos de tu cuenta	Lectura			
PutEventConfiguration	Otorga permiso para crear y actualizar las configuraciones de eventos de un banco de datos de eventos	Escritura	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole
PutEventSelectors	Da permiso para crear y actualizar selectores de eventos para un registro de seguimiento.	Escritura	trail*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutInsightSelectors	Otorga permiso para crear y actualizar los selectores de CloudTrail Insights para un banco de datos de senderos o eventos	Escritura	eventdatastore		
			trail		
PutResourcePolicy	Otorga permiso para adjuntar una política de recursos a un recurso proporcionado.	Escritura	channel		
			dashboard		
			eventdatastore		
RegisterOrganizationDelegatedAdmin	Otorga permiso para registrar una AWS cuenta de miembro de Organizations como administrador delegado	Escritura			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveTags	Otorga permiso para eliminar etiquetas de una ruta, un almacén de datos de eventos, un canal o un panel	Etiquetado	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:TagKeys	
RestoreEventDataStore	Concede permiso para restaurar un almacén de datos de eventos	Escritura	eventdatastore*		
SearchSampleQueries	Otorga permiso para realizar una búsqueda semántica para las consultas de muestra de CloudTrail Lake	Lectura			
StartDashboardRefresh	Otorga permiso para iniciar una actualización en el panel especificado	Escritura	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	Concede permiso para iniciar la ingesta en un almacén de datos de eventos	Escritura	eventdatastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImport	Concede permiso para iniciar una importación de eventos de seguimiento registrados desde un bucket de S3 de origen a un almacén de datos de eventos de destino	Escritura			
StartLogging	Otorga permiso para iniciar la grabación de las llamadas a la AWS API y la entrega de archivos de registro para una ruta	Escritura	trail*		
StartQuery	Concede permiso para iniciar una nueva consulta en almacén de datos de eventos especificado	Escritura	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	Concede permiso para detener la ingesta en un almacén de datos de eventos	Escritura	eventdatastore*		
StopImport	Concede permiso para detener una importación especificada	Escritura			
StopLogging	Otorga permiso para detener la grabación de las llamadas a la AWS API y la entrega de archivos de registro para un seguimiento	Escritura	trail*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateChannel	Da permiso para actualizar un canal.	Escritura	channel*		
UpdateDashboard	Concede permiso para actualizar un panel	Escritura	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery
UpdateEventDataStore	Concede permiso para actualizar un almacén de datos de eventos	Escritura	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceLinkedChannel [solo permiso]	Otorga permiso para actualizar la configuración del canal vinculado al servicio para la entrega de datos de registro a un servicio AWS	Escritura	channel*		
UpdateTrail	Da permiso para actualizar la configuración que especifica la entrega de los archivos de registro.	Escritura	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Tipos de recursos definidos por AWS CloudTrail

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> En el caso de las políticas que controlan el acceso a CloudTrail las acciones, el elemento Recurso siempre está establecido en «*». Para obtener información sobre el uso de los

recursos ARNs en una política de IAM, consulte Cómo AWS CloudTrail funciona con IAM en la Guía del AWS CloudTrail usuario.

Tipos de recurso	ARN	Claves de condición
trail	`arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}`	aws:ResourceTag/${TagKey}
eventdatastore	`arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/${EventDataStoreId}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/${DashboardName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS CloudTrail

AWS CloudTrail define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Claves de condición, recursos y acciones de los AWS CloudTrail datos

AWS CloudTrail Los datos (prefijo de servicio:`cloudtrail-data`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por los datos AWS CloudTrail
- Tipos de recursos definidos por Data AWS CloudTrail
- Claves de condición de los datos AWS CloudTrail

Acciones definidas por los datos AWS CloudTrail

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutAuditEvents	Otorga permiso para incorporar los eventos de su aplicación a Lake CloudTrail	Escritura	channel*		

Tipos de recursos definidos por Data AWS CloudTrail

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> En el caso de las políticas que controlan el acceso a CloudTrail las acciones, el elemento Recurso siempre está establecido en «*». Para obtener información sobre el uso de los recursos ARNs en una política de IAM, consulte Cómo AWS CloudTrail funciona con IAM en la Guía del AWS CloudTrail usuario.

Tipos de recurso	ARN	Claves de condición
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

Claves de condición de los datos AWS CloudTrail

AWS CloudTrail Los datos definen las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon CloudWatch

Amazon CloudWatch (prefijo de servicio:`cloudwatch`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch
- Tipos de recursos definidos por Amazon CloudWatch
- Claves de estado de Amazon CloudWatch

Acciones definidas por Amazon CloudWatch

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetServiceLevelIndicatorReport	Concede permiso para obtener un informe indicador del nivel de servicio por lotes	Lectura			
BatchGetServiceLevelObjectiveBudgetReport	Concede permiso para recuperar un informe de presupuesto objetivo de nivel de servicio por lotes	Lectura	slo*		
CreateServiceLevelObjective	Concede permiso para crear un objetivo de nivel de servicios	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarms	Concede permiso para eliminar una colección de alarmas	Write	alarm*		
DeleteAnomalyDetector	Otorga permiso para eliminar el modelo de detección de anomalías especificado de su cuenta	Escritura			
DeleteDashboards	Otorga permiso para eliminar todos los CloudWatch paneles que especifique	Escritura	dashboard*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteInsightRules	Otorga permiso para eliminar una colección de reglas de información.	Escritura	insight-rule*		
DeleteMetricStream	Otorga permiso para eliminar el flujo de CloudWatch métricas que especifique	Escritura	metric-stream*		
DeleteServiceLevelObjective	Concede permiso para eliminar un objetivo de nivel de servicio	Escritura	slo*		
DescribeAlarmHistory	Otorga permiso para recuperar el historial de la alarma especificada	Read	alarm*		
DescribeAlarms	Otorga permiso para describir todas las alarmas, actualmente propiedad de la cuenta del usuario.	Read	alarm*		
DescribeAlarmsForMetric	Otorga permiso para describir todas las alarmas configuradas en la métrica especificada, actualmente propiedad de la cuenta del usuario	Read			
DescribeAnomalyDetectors	Otorga permiso a los modelos de detección de anomalías que ha creado en su cuenta	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInsightRules	Otorga permiso para describir todas las reglas de información, actualmente propiedad de la cuenta del usuario	Read			
DisableAlarmActions	Otorga permiso para desactivar acciones para una colección de alarmas	Write	alarm*		
DisableInsightRules	Otorga permiso para desactivar una colección de reglas de información	Write	insight-rule*		
EnableAlarmActions	Otorga permiso para habilitar acciones para una colección de alarmas	Write	alarm*		
EnableInsightRules	Otorga permiso para habilitar una colección de reglas de información	Escritura	insight-rule*		
EnableTopologyDiscovery	Otorga permiso para habilitar el descubrimiento de una CloudWatch topología	Escritura			
GenerateQuery	Concede permiso para generar una cadena de consulta de Metrics Insights o Logs Insights a partir de una línea de comandos en lenguaje natural	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateQueryResultsSummary	Otorga permiso para generar un resumen de los resultados de la CloudWatch LogInsights consulta en lenguaje natural mediante la IA generativa	Lectura			
GetDashboard	Otorga permiso para mostrar los detalles del CloudWatch panel de control que especifique	Lectura	dashboard*		
GetInsightRuleReport	Otorga permiso para devolver el informe top-N de colaboradores únicos durante un intervalo de tiempo para una regla de información determinada	Lectura	insight-rule*		
GetMetricData	Otorga permiso para recuperar lotes de datos CloudWatch métricos y realizar cálculos métricos con los datos recuperados	Lectura			
GetMetricStatistics	Otorga permiso para recuperar estadísticas de la métrica especificada	Lectura			
GetMetricStream	Otorga permiso para devolver los detalles de un flujo CloudWatch métrico	Lectura	metric-stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMetricWidgetImage	Otorga permiso para recuperar instantáneas de widgets de métrica	Lectura			
GetService	Concede permiso para recuperar información acerca de un servicio	Lectura	service*		
GetServiceData [solo permiso]	Concede permiso para recuperar datos de un servicio	Lectura	service*		
GetServiceLevelObjective	Concede permiso para recuperar información acerca del objetivo de nivel de servicio	Lectura	slo*		
GetTopologyDiscoveryStatus [solo permiso]	Otorga permiso para recuperar el estado de detección de una CloudWatch topología	Lectura			
GetTopologyMap	Otorga permiso para recuperar un mapa de CloudWatch topología	Lectura			
Link [solo permiso]	Otorga permiso para compartir CloudWatch recursos con una cuenta de supervisión	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDashboards	Otorga permiso para devolver una lista de todos los CloudWatch paneles de su cuenta	Enumeración			
ListEntitiesForMetric [solo permiso]	Otorga permiso para recuperar todas las entidades que emiten una métrica determinada	Enumeración			
ListManagedInsightRules	Concede permiso para enumerar las reglas de información administradas disponibles para un ARN de recurso especificado.	Lectura		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
ListMetricStreams	Otorga permiso para devolver una lista de todos los flujos de CloudWatch métricas de su cuenta	Enumeración			
ListMetrics	Otorga permiso para recuperar una lista de métricas válidas almacenadas para el Cuenta de AWS propietario	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServiceLevelObjectives	Concede permiso para enumerar los objetivos de nivel de servicio	Enumeración			
ListServices	Otorga permiso para enumerar los servicios.	Enumeración			
ListTagsForResource	Otorga permiso para incluir etiquetas para un CloudWatch recurso de Amazon	Enumeración	alarm		
			insight-rule		
			slo		
	ESCENARIO: CloudWatch-Alarm		alarm*		
	ESCENARIO: CloudWatch-InsightRule		insight-rule*		
	ESCENARIO: CloudWatch-ServiceLevelObjective		slo*		
PutAnomalyDetector	Otorga permiso para crear o actualizar un modelo de detección de anomalías para una métrica CloudWatch	Escritura			
PutCompositeAlarm	Otorga permiso para crear o actualizar una alarma compuesta	Escritura	alarm*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	Otorga permiso para crear un CloudWatch panel o actualizar un panel existente si ya existe	Escritura	dashboard*		
PutInsightRule	Otorga permiso para crear una nueva regla de información o remplazar una regla de información existente	Escritura	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutManagedInsightRules	Concede permiso para crear reglas de información administradas.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	Otorga permiso para crear o actualizar una alarma y la asocia a la CloudWatch métrica de Amazon especificada	Escritura	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	Concede permiso para publicar puntos de datos métricos en Amazon CloudWatch	Escritura		cloudwatch:namespace	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutMetricStream	Otorga permiso para crear un flujo de CloudWatch métricas o actualizar un flujo de métricas existente si ya existe	Escritura	metric-stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	Otorga permiso para establecer temporalmente el estado de una alarma con fines de prueba	Escritura	alarm*		
StartMetricStreams	Otorga permiso para iniciar todos los flujos de CloudWatch métricas que especifique	Escritura	metric-stream*		
StopMetricStreams	Otorga permiso para detener todos los flujos de CloudWatch métricas que especifique	Escritura	metric-stream*		
TagResource	Otorga permiso para añadir etiquetas a un CloudWatch recurso de Amazon	Etiquetado	alarm		
			insight-rule		
			slo		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
	ESCENARIO: CloudWatch-Alarm		alarm*		
	ESCENARIO: CloudWatch-InsightRule		insight-rule*		
	ESCENARIO: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Otorga permiso para eliminar una etiqueta de un CloudWatch recurso de Amazon	Etiquetado	alarm		
			insight-rule		
			slo		
				aws:TagKeys	
	ESCENARIO: CloudWatch-Alarm		alarm*		
	ESCENARIO: CloudWatch-InsightRule		insight-rule*		
	ESCENARIO: CloudWatch-ServiceLevelObjective		slo*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceLevelObjective	Concede permiso para actualizar el objetivo de nivel de un servicio	Escritura	slo*		

Tipos de recursos definidos por Amazon CloudWatch

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
alarm	`arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}`	
insight-rule	`arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}`	aws:ResourceTag/${TagKey}
metric-stream	`arn:${Partition}:cloudwatch:${Region}:${Account}:metric-stream/${MetricStreamName}`	aws:ResourceTag/${TagKey}
slo	`arn:${Partition}:cloudwatch:${Region}:${Account}:slo/${SloName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
service	`arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon CloudWatch

Amazon CloudWatch define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función del conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de etiquetas obligatorias en la solicitud.	ArrayOfString
cloudwatch:AlarmActions	Filtra las acciones según las acciones de alarma definidas	ArrayOfString
cloudwatch:namespace	Filtra acciones en función de la presencia de valores de espacio de nombres opcionales	Cadena
cloudwatch:request	Filtra acciones según los grupos de registros especificados en una regla de información	ArrayOfString

Claves de condición	Descripción	Tipo
InsightRuleLogGroups		
cloudwatch:requestManagedResourceARNs	Filtra el acceso según el recurso ARNs especificado en una regla de Insight gestionada	ArrayOfARN

Acciones, recursos y claves de condición de Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights (prefijo de servicio:`applicationinsights`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Application Insights
- Tipos de recursos definidos por Amazon CloudWatch Application Insights
- Claves de condición de Amazon CloudWatch Application Insights

Acciones definidas por Amazon CloudWatch Application Insights

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddWorkload	Concede permiso para agregar una carga de trabajo	Escritura			
CreateApplication	Concede el permiso para crear una aplicación a partir de un grupo de recursos.	Write			
CreateComponent	Concede el permiso para crear un componente a partir de un grupo de recursos.	Write			
CreateLogPattern	Concede el permiso para crear un patrón de registro.	Write			
DeleteApplication	Concede permiso para eliminar una aplicación.	Write			
DeleteComponent	Concede el permiso para eliminar un componente.	Write			
DeleteLogPattern	Concede el permiso para eliminar un patrón de registro.	Write			
DescribeApplication	Concede el permiso para describir una aplicación.	Read			
DescribeComponent	Concede el permiso para describir un componente.	Read			
DescribeComponentConfiguration	Concede el permiso para describir la configuración de un componente.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeComponentConfigurationRecommendation	Concede el permiso para describir la configuración recomendada para el componente de la aplicación.	Read			
DescribeLogPattern	Concede el permiso para describir un patrón de registro.	Read			
DescribeObservation	Concede el permiso para describir una observación.	Read			
DescribeProblem	Concede el permiso para describir un problema.	Read			
DescribeProblemObservations	Concede el permiso para describir la observación en un problema.	Lectura			
DescribeWorkload	Concede permiso para describir una carga de trabajo	Lectura			
Link [solo permiso]	Concede permiso para compartir recursos de Application Insights con una cuenta de monitoreo	Escritura			
ListApplications	Concede el permiso para enumerar todas las aplicaciones.	List			
ListComponents	Concede el permiso para enumerar los componentes de una aplicación.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConfigurationHistory	Concede el permiso para enumerar el historial de configuración.	List			
ListLogPatternSets	Concede el permiso para enumerar conjuntos de patrones de registro para una aplicación.	List			
ListLogPatterns	Concede el permiso para enumerar patrones de registro.	List			
ListProblems	Concede el permiso para enumerar los problemas de una aplicación.	List			
ListTagsForResource	Concede el permiso para obtener una lista de etiquetas para el recurso	Lectura			
ListWorkloads	Concede permiso para enumerar cargas de trabajo	Enumeración			
RemoveWorkload	Concede permiso para elimiinar una carga de trabajo	Escritura			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado		aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Write			
UpdateComponent	Concede el permiso para actualizar una componente.	Write			
UpdateComponentConfiguration	Concede el permiso para actualizar la configuración de un componente.	Write			
UpdateLogPattern	Concede el permiso para actualizar un patrón de registro.	Escritura			
UpdateProblem	Concede permiso para actualizar un problema	Escritura			
UpdateWorkload	Concede permiso para actualizar una carga de trabajo	Escritura			

Tipos de recursos definidos por Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a Amazon CloudWatch Application Insights, especifique `"Resource": "*"` en su política.

Claves de condición de Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals (prefijo de servicio:`application-signals`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Application Signals
- Tipos de recursos definidos por Amazon CloudWatch Application Signals
- Claves de condición de Amazon CloudWatch Application Signals

Acciones definidas por Amazon CloudWatch Application Signals

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetServiceLevelObjectiveBudgetReport	Concede permiso para recuperar un informe de presupuesto objetivo de nivel de servicio por lotes	Lectura	slo*		
BatchUpdateExclusionWindows	Otorga permiso para añadir o eliminar ventanas de exclusión de Amazon CloudWatch SLOs	Escritura	slo*		
CreateServiceLevelObjective	Concede permiso para crear un objetivo de nivel de servicios	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteServiceLevelObjective	Concede permiso para eliminar un objetivo de nivel de servicio	Escritura	slo*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetService	Concede permiso para recuperar información acerca de un servicio	Lectura			
GetServiceLevelObjective	Concede permiso para recuperar información acerca del objetivo de nivel de servicio	Lectura	slo*		
Link [solo permiso]	Otorga permiso para compartir los recursos de Application Signals con una cuenta de monitoreo	Escritura			
ListObservedEntities	Otorga permiso para enumerar entidades asociadas a otras entidades	Enumeración			
ListServiceDependencies	Concede permiso para enumerar dependencias del servicio	Lectura			
ListServiceDependents	Concede permiso para enumerar dependientes del servicio	Lectura			
ListServiceLevelObjectiveExclusionWindows	Otorga permiso para enumerar las ventanas de exclusión de un Amazon CloudWatch SLO	Enumeración	slo*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServiceLevelObjectives	Concede permiso para enumerar los objetivos de nivel de servicio	Enumeración			
ListServiceOperations	Concede permiso para enumerar operaciones del servicio	Lectura			
ListServices	Otorga permiso para enumerar los servicios.	Enumeración			
ListTagsForResource	Otorga permiso para publicar etiquetas para un Amazon CloudWatch SLO	Lectura	slo*		
StartDiscovery	Otorga permiso para permitir el descubrimiento CloudWatch	Escritura			
TagResource	Otorga permiso para añadir etiquetas a un Amazon CloudWatch SLO	Etiquetado	slo*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para desetiquetar un Amazon SLO CloudWatch	Etiquetado	slo*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceLevelObjective	Concede permiso para actualizar el objetivo de nivel de un servicio	Escritura	slo*		

Tipos de recursos definidos por Amazon CloudWatch Application Signals

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
slo	`arn:${Partition}:application-signals:${Region}:${Account}:slo/${SloName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon CloudWatch Evidently

Amazon CloudWatch Evidentemente (prefijo de servicio:`evidently`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Evidentemente
- Tipos de recursos definidos por Amazon CloudWatch Evidentemente
- Claves de estado de Amazon CloudWatch Evidentemente

Acciones definidas por Amazon CloudWatch Evidentemente

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchEvaluateFeature	Concede permiso para enviar una solicitud de característica de evaluación por lotes	Escritura	Feature*		
CreateExperiment	Concede permiso para crear un experimento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeature	Concede permiso para crear una característica	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunch	Concede permiso para crear un lanzamiento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Concede permiso para crear un proyecto	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:GetRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSegment	Otorga permiso para crear un segmento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExperiment	Concede permiso para eliminar un experimento	Escritura	Experiment*		
DeleteFeature	Concede permiso para eliminar una característica	Escritura	Feature*		
DeleteLaunch	Concede permiso para eliminar un lanzamiento	Escritura	Launch*		
DeleteProject	Concede permiso para eliminar un proyecto	Escritura	Project*		
DeleteSegment	Otorga permiso para eliminar un segmento	Escritura	Segment*		
EvaluateFeature	Concede permiso para enviar una solicitud de característica de evaluación	Escritura	Feature*		
GetExperiment	Concede permiso para obtener detalles del experimento	Lectura	Experiment*		
GetExperimentResults	Concede permiso para crear resultados del experimento	Lectura	Experiment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFeature	Concede permiso para obtener detalles de la característica	Lectura	Feature*		
GetLaunch	Concede permiso para obtener detalles del lanzamiento	Lectura	Launch*		
GetProject	Concede permiso para obtener detalles de protección	Lectura	Project*		
GetSegment	Otorga permiso para obtener detalles del segmento	Lectura	Segment*		
ListExperiments	Concede permiso para enumerar experimentos	Lectura			
ListFeatures	Concede permiso para enumerar características	Lectura			
ListLaunches	Concede permiso para enumerar lanzamientos	Lectura			
ListProjects	Concede permiso para enumerar proyectos	Lectura			
ListSegmentReferences	Otorga permiso para enumerar recursos que hacen referencia a un segmento	Lectura			
ListSegments	Otorga permiso para enumerar segmentos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso	Lectura			
PutProjectEvents	Concede permiso para enviar eventos de rendimiento	Escritura	Project*		
StartExperiment	Concede permiso para iniciar un experimento	Escritura	Experiment*		
StartLaunch	Concede permiso para iniciar un lanzamiento	Escritura	Launch*		
StopExperiment	Concede permiso para detener un experimento	Escritura	Experiment*		
StopLaunch	Concede permiso para detener un lanzamiento	Escritura	Launch*		
TagResource	Concede permiso para etiquetar recursos	Etiquetado	Experiment		
			Feature		
			Launch		
			Project		
			Segment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
TestSegmentPattern	Otorga permiso para probar un patrón de segmento	Lectura			
UntagResource	Concede permiso para eliminar etiquetas de recursos	Etiquetado	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:TagKeys	
UpdateExperiment	Concede permiso para actualizar un experimento	Escritura	Experiment*		
UpdateFeature	Concede permiso para actualizar la característica	Escritura	Feature*		
UpdateLaunch	Concede permiso para actualizar un perfil de lanzamiento	Escritura	Launch*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateProject	Concede permiso para actualizar un proyecto	Escritura	Project*		iam:CreateServiceLinkedRole iam:GetRole
UpdateProjectDataDelivery	Concede permiso para actualizar la entrega de datos del proyecto	Escritura	Project*		

Tipos de recursos definidos por Amazon CloudWatch Evidentemente

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Project	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey}
Feature	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/feature/${FeatureName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Experiment	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/experiment/${ExperimentName}`	aws:ResourceTag/${TagKey}
Launch	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/launch/${LaunchName}`	aws:ResourceTag/${TagKey}
Segment	`arn:${Partition}:evidently:${Region}:${Account}:segment/${SegmentName}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon CloudWatch Evidentemente

CloudWatch Evidentemente, Amazon define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas por las que se pasa la solicitud en nombre del principal de IAM.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas con el recurso que hace la solicitud en nombre del principal de IAM.	Cadena
aws:TagKeys	Filtra el acceso por las etiquetas por las que se pasa en la solicitud en nombre del principal de IAM.	ArrayOfString

Claves de condición, recursos y acciones de Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor (prefijo de servicio:`internetmonitor`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Internet Monitor
- Tipos de recursos definidos por Amazon CloudWatch Internet Monitor
- Claves de condición de Amazon CloudWatch Internet Monitor

Acciones definidas por Amazon CloudWatch Internet Monitor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMonitor	Otorga permiso para crear un monitor	Escritura	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMonitor	Otorga permiso para eliminar un monitor	Escritura	Monitor*		
GetHealthEvent	Otorga permiso para obtener información acerca del evento de estado para un monitor especificado	Lectura	Monitor*		
GetInternetEvent	Concede permiso para obtener información sobre un evento específico de Internet	Lectura	InternetEvent*		
GetMonitor	Otorga permiso para obtener información sobre un monitor	Lectura	Monitor*		
GetQueryResults	Concede permiso para obtener los resultados de una consulta de datos para un monitor	Lectura	Monitor*		
GetQueryStatus	Concede permiso para obtener el estado de una consulta de datos para un monitor	Lectura	Monitor*		
Link [solo permiso]	Concede permiso para compartir recursos de Internet Monitor con una cuenta de supervisión	Escritura			
ListHealthEvents	Otorga permiso para enumerar todos los eventos de estado para un monitor	Enumeración	Monitor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListInternetEvents	Concede permiso para enumerar todos los eventos de Internet	Enumeración			
ListMonitors	Otorga permiso para enumerar todos los monitores de una cuenta y sus estados	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	Monitor*		
StartQuery	Concede permiso para iniciar una consulta de datos para un monitor	Lectura	Monitor*		
StopQuery	Concede permiso para detener una consulta de datos para un monitor	Lectura	Monitor*		
TagResource	Otorga permiso para agregar etiquetas a un recurso.	Etiquetado	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	Monitor*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMonitor	Otorga permiso para actualizar un monitor	Escritura	Monitor*		

Tipos de recursos definidos por Amazon CloudWatch Internet Monitor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
HealthEvent	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}/health-event/${EventId}`	aws:ResourceTag/${TagKey}
Monitor	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
InternetEvent	`arn:${Partition}:internetmonitor::${Account}:internet-event/${InternetEventId}`	

Claves de condición de Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar

más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon CloudWatch Logs

Amazon CloudWatch Logs (prefijo de servicio:`logs`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Logs
- Tipos de recursos definidos por Amazon CloudWatch Logs
- Claves de condición de Amazon CloudWatch Logs

Acciones definidas por Amazon CloudWatch Logs

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateKmsKey	Otorga permiso para asociar la AWS clave maestra del cliente (CMK) del Servicio de administración de claves (AWS KMS) especificada al grupo de registros especificado	Escritura	log-group*		
CancelExportTask	Otorga permiso para cancelar una tarea de exportación si se encuentra en estado PENDING (Pendiente) o RUNNING (En ejecución)	Escritura			
CreateDelivery	Concede permiso para crear una entrega que conecte una fuente de entrega a un destino de entrega	Escritura	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateExportTask	Otorga permiso para crear un ExportTask que le permite exportar datos de manera eficiente desde un grupo de registros a su bucket de Amazon S3	Escritura	log-group*		
CreateLogAnomalyDetector	Otorga permiso para crear un detector de anomalías de registro	Escritura	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogDelivery [solo permiso]	Otorga permiso para crear la entrega de registros	Escritura			
CreateLogGroup	Otorga permiso para crear un nuevo grupo de registro con el nombre especificado	Escritura	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	Otorga permiso para crear un nuevo flujo de registro con el nombre especificado	Escritura	log-stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccountPolicy	Otorga permiso para eliminar una política de cuentas	Escritura			
DeleteDataProtectionPolicy	Otorga permiso para eliminar una política de protección de datos adjunta a un grupo de registro	Escritura	log-group*		
DeleteDelivery	Concede permiso para eliminar una entrega	Escritura	delivery*		
DeleteDeliveryDestination	Concede permiso para eliminar un destino de entrega una vez que se eliminen todas las entregas asociadas	Escritura	delivery-destination*		
DeleteDeliveryDestinationPolicy	Concede permiso para eliminar una política de destino de entrega asociada a un destino de entrega	Escritura	delivery-destination*		
DeleteDeliverySource	Concede permiso para eliminar un origen de entrega una vez que se eliminen todos los envíos asociados	Escritura	delivery-destination*		
DeleteDestination	Otorga permiso para eliminar el destino con el nombre especificado	Escritura	destination*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIndexPolicy	Otorga permiso para eliminar una política de indexación asociada a un grupo de registros	Escritura			
DeleteIntegration	Otorga permiso para eliminar la integración	Escritura			
DeleteLogAnomalyDetector	Otorga permiso para eliminar un detector de anomalías de registro	Escritura	anomaly-detector*		
DeleteLogDelivery [solo permiso]	Otorga permiso para eliminar la información de entrega de registros de la entrega de registros especificada	Escritura			
DeleteLogGroup	Otorga permiso para eliminar el grupo de registro con el nombre especificado	Escritura	log-group*		
DeleteLogStream	Otorga permiso para eliminar un flujo de registro	Escritura	log-stream*		
DeleteMetricFilter	Otorga permiso para eliminar un filtro de métricas asociado al grupo de registro especificado	Escritura	log-group*		
DeleteQueryDefinition	Otorga permiso para eliminar una definición de consulta de CloudWatch Logs Insights guardada	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcePolicy	Otorga permiso para eliminar una política de recursos de esta cuenta	Administración de permisos			
DeleteRetentionPolicy	Otorga permiso para eliminar la política de retención del grupo de registro especificado	Escritura	log-group*		
DeleteSubscriptionFilter	Otorga permiso para eliminar un filtro de suscripción asociado al grupo de registro especificado	Escritura	log-group*		
DeleteTransformer	Otorga permiso para eliminar un transformador asociado al grupo de registros especificado	Escritura	log-group*		
DescribeAccountPolicies	Otorga permiso para recuperar las políticas de la cuenta	Enumeración			
DescribeConfigurationTemplates	Concede permiso para recuperar una lista de plantillas de configuración de los tipos de registro disponibles	Enumeración			
DescribeDeliveries	Concede permiso para recuperar una lista de entregas de una cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDeliveryDestinations	Concede permisos para recuperar una lista de destinos de entrega dentro de una cuenta	Enumeración			
DescribeDeliverySources	Concede permiso para recuperar una lista de origen de entrega en una cuenta	Enumeración			
DescribeDestinations	Otorga permiso para devolver todos los destinos asociados a la Cuenta de AWS realización de la solicitud	Enumeración			
DescribeExportTasks	Otorga permiso para devolver todas las tareas de exportación asociadas a la Cuenta de AWS realización de la solicitud	Enumeración			
DescribeFieldIndexes	Otorga permiso para devolver todos los atributos de indexación adjuntos a los grupos de registros	Enumeración			
DescribeIndexPolicies	Otorga permiso para devolver todas las políticas de indexación adjuntas a los grupos de registros	Enumeración			
DescribeLogGroups	Otorga permiso para devolver todos los grupos de registros asociados Cuenta de AWS a la solicitud	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeLogStreams	Otorga permiso para devolver todos los flujos de registro que están asociados al grupo de registro especificado	Enumeración	log-group *		
DescribeMetricFilters	Otorga permiso para devolver todos los filtros de métricas asociados al grupo de registro especificado	Enumeración	log-group *		
DescribeQueries	Otorga permiso para devolver una lista de las consultas de CloudWatch Logs Insights que están programadas, en ejecución o que se han ejecutado recientemente en esta cuenta	Enumeración			
DescribeQueryDefinitions	Otorga permiso para devolver una lista paginada de las definiciones de consultas de CloudWatch Logs Insights guardadas	Enumeración			
DescribeResourcePolicies	Otorga permiso para devolver todas las políticas de recursos en esta cuenta	Enumeración			
DescribeSubscriptionFilters	Otorga permiso para devolver todos los filtros de suscripción asociados al grupo de registro especificado	Enumeración	log-group *		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateKmsKey	Otorga permiso para desasociar la AWS clave maestra del cliente (CMK) del Servicio de administración de claves (AWS KMS) asociada del grupo de registros especificado	Escritura	log-group*		
FilterLogEvents	Otorga permiso para recuperar los eventos de registro, que se filtran de forma opcional por un patrón de filtro del grupo de registro especificado	Lectura	log-group*		
GetDataProtectionPolicy	Otorga permiso para recuperar una política de protección de datos adjunta a un grupo de registro	Lectura	log-group*		
GetDelivery	Concede permiso para recuperar una entrega única	Lectura	delivery*		
GetDeliveryDestination	Concede permiso para recuperar un único destino de entrega	Lectura	delivery-destination*		
GetDeliveryDestinationPolicy	Concede permiso para recuperar una política de destino de entrega adjunta a un destino de entrega	Lectura	delivery-destination*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeliverySource	Concede permiso para recuperar un origen de entrega única	Lectura	delivery-source*		
GetIntegration	Otorga permiso para recuperar una sola integración	Lectura			
GetLogAnomalyDetector	Otorga permiso para obtener una lista de detectores de anomalías de registro	Lectura	anomaly-detector*		
GetLogDelivery [solo permiso]	Otorga permiso para obtener la información de entrega de registros de la entrega de registros especificada	Lectura			
GetLogEvents	Otorga permiso para recuperar los eventos de registro del flujo de registro especificado	Lectura	log-stream*		
GetLogGroupFields	Otorga permiso para devolver una lista de los campos que se incluyen en los eventos de registro en el grupo de registro especificado, junto con el porcentaje de eventos de registro que contiene cada campo	Lectura	log-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLogRecord	Otorga permiso para recuperar todos los campos y valores de un único evento de registro	Lectura	log-group *		
GetQueryResults	Otorga permiso para devolver los resultados de la consulta especificada	Lectura	log-group *		
GetTransformer	Otorga permiso para devolver el transformador asociado al grupo de registros especificado	Lectura	log-group *		
Link [solo permiso]	Otorga permiso para compartir CloudWatch recursos con una cuenta de supervisión	Escritura			
ListAnomalies	Otorga permiso para enumerar todas las anomalías detectadas al Cuenta de AWS realizar la solicitud	Enumeración	anomaly-detector		
ListEntitiesForLogGroup [solo permiso]	Otorga permiso para recuperar todas las entidades asociadas al grupo de registros	Enumeración			
ListIntegrations	Otorga permiso para enumerar todas las integraciones asociadas a la Cuenta de AWS realización de la solicitud	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLogAnomalyDetectors	Otorga permiso para devolver todos los detectores de anomalías asociados a la Cuenta de AWS solicitud	Enumeración	anomaly-detector		
ListLogDeliveries [solo permiso]	Otorga permiso para enumerar todas las entregas de registros de una fuente de and/or registro de cuentas específica	Enumeración			
ListLogGroups	Otorga permiso para devolver todos los grupos de registros asociados Cuenta de AWS a la solicitud	Enumeración			
ListLogGroupsForEntity [solo permiso]	Otorga permiso para recuperar todos los grupos de registros asociados a la entidad	Enumeración			
ListLogGroupsForQuery	Otorga permiso para devolver todos los grupos de registros asociados a la consulta especificada	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso especificado	Enumeración	anomaly-detector		
			delivery		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	Otorga permiso para enumerar las etiquetas para el grupo de registro especificado	Enumeración	log-group *		
PutAccountPolicy	Otorga permiso para adjuntar una política de cuenta	Escritura			
PutDataProtectionPolicy	Otorga permiso para adjuntar una política de protección de datos para detectar y eliminar información confidencial de los eventos de registro	Escritura	log-group *		
PutDeliveryDestination	Otorga permiso a create/update un destino de entrega	Escritura	delivery-destination*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	Concede permiso para adjuntar una política de destino de entrega a un destino de entrega	Escritura	delivery-destination*		
PutDeliverySource	Otorga permiso a create/update una fuente de entrega	Escritura	delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	
PutDestination	Otorga permiso para crear o actualizar un destino	Escritura	destination*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	Otorga permiso para crear o actualizar una política de acceso asociada a un destino existente	Escritura	destination*		
PutIndexPolicy	Otorga permiso para adjuntar una política de indexación a nivel de grupo de registros para optimizar las búsquedas y consultas	Escritura			
PutIntegration	Otorga permiso para crear una integración entre los registros de Cloudwatch y opensearch	Escritura			
PutLogEvents	Otorga permiso para cargar un lote de eventos de registro en el flujo de registro especificado	Escritura	log-stream*		
PutMetricFilter	Otorga permiso para crear o actualizar un filtro de métricas y lo asocia al grupo de registro especificado	Escritura	log-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutQueryDefinition	Otorga permiso para crear o actualizar una definición de consulta	Escritura			
PutResourcePolicy	Otorga permiso para crear o actualizar una política de recursos que permita a otros AWS servicios colocar los eventos de registro en esta cuenta	Administración de permisos			
PutRetentionPolicy	Otorga permiso para configurar la retención del grupo de registro especificado	Escritura	log-group *		
PutSubscriptionFilter	Otorga permiso para crear o actualizar un filtro de suscripciones y lo asocia al grupo de registro especificado	Escritura	log-group *		iam:PassRole
			destination		
PutTransformer	Otorga permiso para crear o actualizar un transformador y lo asocia al grupo de registros especificado	Escritura	log-group *		
StartLiveTail	Otorga permiso para iniciar una sesión de Live Tail en CloudWatch Logs	Lectura	log-group *		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartQuery	Otorga permiso para programar una consulta de un grupo de CloudWatch registros mediante Logs Insights	Lectura	log-group *		
StopLiveTail [solo permiso]	Concede permiso para detener una sesión de Live Tail que está en curso	Lectura			
StopQuery	Otorga permiso para detener una consulta de CloudWatch Logs Insights que está en curso	Lectura			
TagLogGroup	Otorga permiso para agregar o actualizar las etiquetas especificadas del grupo de registro especificado	Etiquetado	log-group *		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Otorga permiso para agregar o actualizar las etiquetas especificadas para el recurso especificado	Etiquetado	anomaly-detector		
			delivery		
			delivery-destination		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			delivery-source		
			destination		
			log-group		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	Otorga permiso para probar el patrón de filtro de un filtro de métricas y compararlo con una muestra de los mensajes de eventos de registro	Lectura			
TestTransformer	Otorga permiso para probar el transformador con una muestra de mensajes de eventos de registro	Lectura			
Unmask [solo permiso]	Otorga permiso para recuperar eventos de registro desenmascarados que se han eliminado con una política de protección de datos	Lectura	log-group *		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagLogGroup	Otorga permiso para quitar las etiquetas especificadas del grupo de registro especificado	Etiquetado	log-group*		
				aws:TagKeys	
UntagResource	Otorga permiso para quitar las etiquetas especificadas de los recursos especificados	Etiquetado	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
				aws:TagKeys	
UpdateAnomaly	Otorga permiso para actualizar una anomalía informada por un detector de anomalías de registro	Escritura	anomaly-detector*		
UpdateDeliveryConfiguration	Concede permiso para actualizar la configuración relacionada con una entrega	Escritura	delivery*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateLogAnomalyDetector	Otorga permiso para actualizar un detector de anomalías de registro	Escritura	anomaly-detector*		
UpdateLogDelivery [solo permiso]	Otorga permiso para actualizar la información de entrega de registros de la entrega de registros especificada	Escritura			

Tipos de recursos definidos por Amazon CloudWatch Logs

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
log-group	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}	aws:ResourceTag/${TagKey}
log-stream	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}	aws:ResourceTag/${TagKey}
destination	arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}	aws:ResourceTag/${TagKey}
delivery-source	arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}	aws:ResourceTag/${TagKey}
delivery	arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}	aws:ResourceTag/${TagKey}
delivery-destination	arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}	aws:ResourceTag/${TagKey}
anomaly-detector	arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}	aws:ResourceTag/${TagKey}

Claves de condición de Amazon CloudWatch Logs

Amazon CloudWatch Logs define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
logs:DeliveryDestinationResourceArn	Filtra el acceso por el ARN de destino del registro que se incluye en la solicitud	ARN
logs:LogGenerating ResourceArns	Filtra el acceso por el recurso generador de registros ARNs ingresado en la solicitud	ArrayOfARN

Claves de condición, recursos y acciones de Amazon CloudWatch Network Synthetic Monitor

Amazon CloudWatch Network Synthetic Monitor (prefijo de servicio:`networkmonitor`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Network Synthetic Monitor
- Tipos de recursos definidos por Amazon CloudWatch Network Synthetic Monitor
- Claves de condición de Amazon CloudWatch Network Synthetic Monitor

Acciones definidas por Amazon CloudWatch Network Synthetic Monitor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMonitor	Otorga permiso para crear un monitor	Escritura	monitor*		
CreateProbe	Concede permiso para crear un sondeo	Escritura			
DeleteMonitor	Otorga permiso para eliminar un monitor	Escritura	monitor*		
DeleteProbe	Concede permiso para eliminar un sondeo	Escritura	probe*		
GetMonitor	Otorga permiso para obtener información sobre un monitor	Lectura	monitor*		
GetProbe	Concede permiso para obtener información sobre un sondeo	Lectura	probe*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMonitors	Otorga permiso para enumerar todos los monitores de una cuenta y sus estados	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	monitor		
			probe		
TagResource	Otorga permiso para agregar etiquetas a un recurso.	Etiquetado	monitor		
			probe		
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	monitor		
			probe		
				aws:TagKeys	
UpdateMonitor	Otorga permiso para actualizar un monitor	Escritura	monitor*		
UpdateProbe	Concede permiso para actualizar un sondeo	Escritura	probe*		

Tipos de recursos definidos por Amazon CloudWatch Network Synthetic Monitor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
monitor	`arn:${Partition}:networkmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
probe	`arn:${Partition}:networkmonitor:${Region}:${Account}:probe/${ProbeId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon CloudWatch Network Synthetic Monitor

Amazon CloudWatch Network Synthetic Monitor define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra las acciones mediante las claves de etiqueta en la solicitud.	ArrayOfString

Claves de condición, recursos y acciones de Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager (prefijo de servicio:`oam`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Observability Access Manager
- Tipos de recursos definidos por Amazon CloudWatch Observability Access Manager
- Claves de condición de Amazon CloudWatch Observability Access Manager

Acciones definidas por Amazon CloudWatch Observability Access Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLink	Otorga permiso para crear un enlace entre una cuenta de monitoreo y una cuenta de origen para el monitoreo entre cuentas	Escritura	Sink*		oam:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				oam:ResourceTypes	
CreateSink	Otorga permiso para crear un receptor en una cuenta de modo que pueda utilizarse como cuenta de monitoreo para el monitoreo entre cuentas	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	Otorga permiso para eliminar un enlace entre una cuenta de monitoreo y una cuenta de origen para el monitoreo entre cuentas	Escritura	Link*		
				aws:ResourceTag/${TagKey}	
DeleteSink	Otorga permiso para eliminar un receptor de monitoreo entre cuentas de una cuenta de monitoreo	Escritura	Sink*		
				aws:ResourceTag/${TagKey}	
GetLink	Otorga permiso para recuperar la información completa sobre un enlace de monitoreo entre cuentas	Lectura	Link*		
				aws:ResourceTag/${TagKey}	
GetSink	Otorga permiso para recuperar la información completa sobre un receptor de monitoreo entre cuentas	Lectura	Sink*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSinkPolicy	Otorga permiso para recuperar información de la política de IAM para un receptor de monitoreo entre cuentas	Lectura	Sink*		
				aws:ResourceTag/${TagKey}	
ListAttachedLinks	Otorga permiso para recuperar una lista de enlaces que están vinculados para un receptor de monitoreo entre cuentas	Lectura	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	Otorga permiso para recuperar los enlaces ARNs de supervisión multicuenta de esta cuenta	Lectura			
ListSinks	Otorga permiso para recuperar los ARNs puntos de monitoreo multicuenta de esta cuenta	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	Link		
			Sink		
PutSinkPolicy	Otorga permiso para crear o actualizar la política de IAM para un receptor de monitoreo entre cuentas	Escritura	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	Link		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	Link		
			Sink		
				aws:TagKeys	
UpdateLink	Otorga permiso para actualizar un enlace existente entre una cuenta de monitoreo y una cuenta de origen	Escritura	Link*		
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

Tipos de recursos definidos por Amazon CloudWatch Observability Access Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Link	`arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}`	aws:ResourceTag/${TagKey}
Sink	`arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
oam:ResourceTypes	Filtra el acceso por la presencia de tipos de recursos en la solicitud	ArrayOfString

Acciones, recursos y claves de condición del Servicio de administración de Amazon CloudWatch Observability

Amazon CloudWatch Observability Admin Service (prefijo de servicio:`observabilityadmin`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de administración de Amazon CloudWatch Observability
- Tipos de recursos definidos por el servicio de administración de Amazon CloudWatch Observability
- Claves de condición del servicio de administración de Amazon CloudWatch Observability

Acciones definidas por el servicio de administración de Amazon CloudWatch Observability

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTelemetryEvaluationStatus	Otorga permiso para recuperar el estado de la función Telemetry Config de la cuenta	Lectura			
GetTelemetryEvalua	Otorga permiso para recuperar el estado de la	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
tionStatusForOrganization	función Telemetry Config de la organización				
ListResourceTelemetry	Otorga permiso para recuperar las configuraciones de telemetría de los recursos asociados a la cuenta	Lectura			
ListResourceTelemetryForOrganization	Otorga permiso para recuperar las configuraciones de telemetría de los recursos asociados a las cuentas de la organización	Lectura			
StartTelemetryEvaluation	Otorga permiso para iniciar la función Telemetry Config de la cuenta	Escritura			
StartTelemetryEvaluationForOrganization	Otorga permiso para iniciar la función Telemetry Config para la organización	Escritura			
StopTelemetryEvaluation	Otorga permiso para detener la función Telemetry Config de la cuenta	Escritura			
StopTelemetryEvaluationForOrganization	Otorga permiso para detener la función Telemetry Config para la organización	Escritura			

Tipos de recursos definidos por el servicio de administración de Amazon CloudWatch Observability

El servicio de administración de Amazon CloudWatch Observability no admite la especificación de un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso al Servicio de administración de Amazon CloudWatch Observability, especifíquelo `"Resource": "*"` en su política.

Claves de condición del servicio de administración de Amazon CloudWatch Observability

CloudWatch Observability Admin no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones de AWS CloudWatch RUM

AWS CloudWatch RUM (prefijo de servicio:`rum`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por RUM AWS CloudWatch
- Tipos de recursos definidos por AWS CloudWatch RUM
- Claves de condición para AWS CloudWatch RUM

Acciones definidas por RUM AWS CloudWatch

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchCreateRumMetricDefinitions	Otorga permiso para crear definiciones métricas de RUM	Escritura	AppMonitorResource*		
BatchDeleteRumMetricDefinitions	Otorga permiso para eliminar definiciones métricas de RUM	Escritura	AppMonitorResource*		
BatchGetRumMetricDefinitions	Otorga permiso para obtener definiciones métricas de RUM	Lectura	AppMonitorResource*		
CreateAppMonitor	Otorga permiso para crear metadatos de appMonitor.	Escritura	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppMonitor	Otorga permiso para eliminar metadatos de appMonitor.	Escritura	AppMonitorResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcePolicy	Otorga permiso para eliminar una política de recursos adjunta a un monitor de aplicaciones	Escritura	AppMonitorResource*		
DeleteRumMetricsDestination	Otorga permiso para eliminar destinos de métricas de RUM	Escritura	AppMonitorResource*		
GetAppMonitor	Otorga permiso para obtener metadatos de appMonitor.	Lectura	AppMonitorResource*		
GetAppMonitorData	Otorga permiso para obtener datos de AppMonitor.	Lectura	AppMonitorResource*		
GetResourcePolicy	Otorga permiso para recuperar una política de recursos adjunta a un monitor de aplicaciones	Lectura	AppMonitorResource*		
ListAppMonitors	Otorga permiso para enumerar metadatos de appMonitor.	Enumeración			
ListRumMetricsDestinations	Otorga permiso para enumerar destinos de métricas de RUM	Lectura	AppMonitorResource*		
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResourcePolicy	Otorga permiso para adjuntar una política de recursos a un monitor de aplicaciones	Escritura	AppMonitorResource*		
PutRumEvents	Otorga permiso para colocar eventos de RUM para appMonitor.	Escritura	AppMonitorResource*		
PutRumMetricsDestination	Otorga permiso para colocar destinos de métricas de RUM	Escritura	AppMonitorResource*		
TagResource	Concede permiso para etiquetar recursos	Etiquetado	AppMonitorResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de recursos	Etiquetado	AppMonitorResource*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAppMonitor	Otorga permiso para actualizar metadatos de appMonitor.	Escritura	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
UpdateRumMetricDefinition	Otorga permiso para actualizar una definición de métrica de RUM	Escritura	AppMonitorResource*		

Tipos de recursos definidos por AWS CloudWatch RUM

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AppMonitorResource	`arn:${Partition}:rum:${Region}:${Account}:appmonitor/${Name}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS CloudWatch RUM

AWS CloudWatch RUM define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas por las que se pasa la solicitud en nombre del principal de IAM.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas con el recurso que hace la solicitud en nombre del principal de IAM.	Cadena
aws:TagKeys	Filtra el acceso por las etiquetas por las que se pasa en la solicitud en nombre del principal de IAM.	ArrayOfString

Acciones, recursos y claves de condición de Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics (prefijo de servicio:`synthetics`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CloudWatch Synthetics
- Tipos de recursos definidos por Amazon CloudWatch Synthetics

- Claves de estado de Amazon CloudWatch Synthetics

Acciones definidas por Amazon CloudWatch Synthetics

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateResource	Concede permiso para asociar un recurso a un grupo	Escritura	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCanary	Otorga permiso para crear un canary	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroup	Concede permiso para crear un grupo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCanary	Otorga permiso para eliminar un canary. Amazon Synthetics elimina todos los recursos, excepto la función Lambda y	Escritura	canary*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	las alarmas, si ha creado una. CloudWatch			aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteGroup	Concede permiso para eliminar un grupo	Escritura	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Otorga permiso para enumerar información de todos los valores controlados.	Read		synthetics:Names	
DescribeCanariesLastRun	Otorga permiso para enumerar información sobre la última ejecución de prueba asociada a todos los valores controlados.	Read		synthetics:Names	
DescribeRuntimeVersions	Otorga permiso para mostrar información sobre las versiones de tiempo de ejecución de los canary de Synthetics.	Lectura			
DisassociateResource		Escritura	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para disociar un recurso de un recurso			aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	Concede permiso para ver los detalles de un valor controlado	Lectura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Otorga permiso para enumerar información de todas las ejecuciones de prueba asociadas a un canary.	Lectura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	Concede permiso para visualizar los detalles de un grupo	Lectura	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssociatedGroups	Concede permiso para enumerar información de todos los grupos asociados de un valor controlado	Enumeración	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	Concede permiso para enumerar información sobre valores controlados en un grupo	Enumeración	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroups	Concede permiso para enumerar información de todos los grupos	Enumeración			
ListTagsForResource	Concede permiso para enumerar todas las etiquetas y valores asociados a un recurso	Lectura	canary		
			group		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCanary	Otorga permiso para iniciar un canario, de modo que Amazon CloudWatch Synthetics comience a monitorear un sitio web	Escritura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StartCanaryDryRun	Otorga permiso para iniciar un simulacro canario, de modo que Amazon CloudWatch Synthetics pueda ejecutar una ejecución de prueba de un canario con los parámetros proporcionados	Escritura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	Otorga permiso para detener un canary.	Escritura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso.	Etiquetado	canary		
			group		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	canary		
			group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Otorga permiso para actualizar un canary.	Escritura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por Amazon CloudWatch Synthetics

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
canary	`arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}`	aws:ResourceTag/${TagKey}
group	`arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString
synthetics:Names	Filtra el acceso en función del nombre del valor controlado	ArrayOfString

Acciones, recursos y claves de condición para AWS CodeArtifact

AWS CodeArtifact (prefijo de servicio:`codeartifact`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodeArtifact
- Tipos de recursos definidos por AWS CodeArtifact
- Claves de condición de AWS CodeArtifact

Acciones definidas por AWS CodeArtifact

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateExternalConnection	Otorga permiso para agregar una conexión externa a un repositorio	Write	repository*		
AssociateWithDownstreamRepository	Otorga permiso para asociar un repositorio existente como repositorio ascendente a otro repositorio	Escritura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CopyPackageVersions	Otorga permiso para copiar versiones de paquetes de un repositorio a otro repositorio del mismo dominio	Escritura	package* repository*		
CreateDomain	Otorga permiso para crear un nuevo dominio	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackageGroup	Concede permiso para crear un grupo de paquetes	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepository	Otorga permiso para crear un nuevo repositorio	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDomain	Concede permiso para eliminar un dominio	Write	domain*		
DeleteDomainPermissionsPolicy	Otorga permiso para eliminar la política de recursos establecida en un dominio	Administración de permisos	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePackage	Otorga permiso para eliminar un paquete	Escritura	package*		
DeletePackageGroup	Concede permiso para eliminar un grupo de paquetes	Escritura	package-group*		
DeletePackageVersions	Otorga permiso para eliminar versiones de paquetes	Write	package*		
DeleteRepository	Otorga permiso para eliminar un repositorio	Write	repository*		
DeleteRepositoryPermissionsPolicy	Otorga permiso para eliminar el conjunto de políticas de recursos de un repositorio	Permissions management	repository*		
DescribeDomain	Otorga permiso para devolver información acerca de un dominio	Lectura	domain*		
DescribePackage	Otorga permiso para recuperar información acerca de un paquete	Lectura	package*		
DescribePackageGroup	Concede permiso para devolver información detallada sobre un grupo de paquetes	Lectura	package-group*		
DescribePackageVersion	Otorga permiso para devolver información acerca de una versión de paquete	Read	package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRepository	Otorga permiso para devolver información detallada acerca de un repositorio	Read	repository*		
DisassociateExternalConnection	Otorga permiso para desasociar una conexión externa de un repositorio	Write	repository*		
DisposePackageVersions	Otorga permiso para establecer el estado de versiones de paquetes en Eliminado y eliminar sus recursos	Escritura	package*		
GetAssociatedPackageGroup	Concede permiso para devolver el grupo de paquetes asociado de un paquete	Lectura	package-group*		
GetAuthorizationToken	Otorga permiso para generar un token de autenticación temporal para acceder a repositorios de un dominio	Read	domain*		
GetDomainPermissionsPolicy	Otorga permiso para devolver la política de recursos de un dominio	Read	domain*		
GetPackageVersionAsset	Otorga permiso para devolver un recurso (o archivo) que forma parte de una versión de paquete	Read	package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPackageVersionReadme	Otorga permiso para devolver el archivo readme de una versión de paquete	Read	package*		
GetRepositoryEndpoint	Otorga permiso para devolver un punto de enlace a un repositorio	Read	repository*		
GetRepositoryPermissionsPolicy	Otorga permiso para devolver la política de recursos de un repositorio	Lectura	repository*		
ListAllowedRepositoriesForGroup	Concede permiso para enumerar los repositorios permitidos para un grupo de paquetes	Enumeración	package-group*		
ListAssociatedPackages	Concede permiso para enumerar los paquetes asociados a un grupo de paquetes	Enumeración	package-group*		
ListDomains	Otorga permiso para enumerar los dominios del usuario actual Cuenta de AWS	Enumeración			
ListPackageGroups	Concede permiso para enumerar los grupos de paquetes de un dominio	Enumeración	domain*		
ListPackageVersionAssets	Otorga permiso para mostrar una lista de los recursos de una versión de paquete	List	package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPackageVersionDependencies	Otorga permiso para mostrar una lista de las dependencias directas de una versión de paquete	List	package*		
ListPackageVersions	Otorga permiso para mostrar una lista de las versiones de un paquete	List	package*		
ListPackages	Otorga permiso para mostrar una lista de los paquetes de un repositorio	List	repository*		
ListRepositories	Otorga permiso para mostrar una lista de los repositorios administrados por la cuenta de llamada	List			
ListRepositoriesInDomain	Otorga permiso para mostrar una lista de los repositorios de un dominio	Enumeración	domain*		
ListSubPackageGroups	Concede permiso para enumerar los grupos de paquetes secundarios de un grupo de paquetes principal	Enumeración	package-group*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un CodeArtifact recurso	Enumeración	domain		
			package-group		
			repository		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PublishPackageVersion	Otorga permiso para publicar recursos y metadatos en el punto de enlace de un repositorio	Write	package*		
PutDomainPermissionsPolicy	Otorga permiso para asociar una política de recursos a un dominio	Write	domain*		
PutPackageMetadata	Otorga permiso para agregar, modificar o eliminar metadatos del paquete mediante el punto de enlace de un repositorio	Escritura	package*		
PutPackageOriginConfiguration	Otorga permiso para establecer la configuración de origen para un paquete	Escritura	package*		
PutRepositoryPermissionsPolicy	Otorga permiso para asociar una política de recursos a un repositorio	Write	repository*		
ReadFromRepository	Otorga permiso para devolver recursos y metadatos del paquete desde el punto de enlace de un repositorio	Lectura	repository*		
TagResource	Otorga permiso para etiquetar un CodeArtifact recurso	Etiquetado	domain		
			package-group		
			repository		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una etiqueta de un CodeArtifact recurso	Etiquetado	domain		
			package-group		
			repository		
				aws:TagKeys	
UpdatePackageGroup	Concede permiso para modificar las propiedades de un grupo de paquetes	Escritura	package-group*		
UpdatePackageGroupOriginConfiguration	Concede permiso para modificar la configuración del origen de paquetes de un grupo de paquetes	Escritura	package-group*		
UpdatePackageVersionsStatus	Otorga permiso para modificar el estado de una o varias versiones de un paquete	Write	package*		
UpdateRepository	Otorga permiso para modificar las propiedades de un repositorio	Escritura	repository*		

Tipos de recursos definidos por AWS CodeArtifact

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> El ARN del recurso de grupos de paquetes debe utilizar un patrón de grupo de paquetes codificado.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:codeartifact:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}
repository	`arn:${Partition}:codeartifact:${Region}:${Account}:repository/${DomainName}/${RepositoryName}`	aws:ResourceTag/${TagKey}
package-group	`arn:${Partition}:codeartifact:${Region}:${Account}:package-group/${DomainName}${EncodedPackageGroupPattern}`	aws:ResourceTag/${TagKey}
package	`arn:${Partition}:codeartifact:${Region}:${Account}:package/${DomainName}/${RepositoryName}/${PackageFormat}/${PackageNamespace}/${PackageName}`	

Claves de condición de AWS CodeArtifact

AWS CodeArtifact define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon CodeCatalyst

Amazon CodeCatalyst (prefijo de servicio:`codecatalyst`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CodeCatalyst
- Tipos de recursos definidos por Amazon CodeCatalyst
- Claves de estado de Amazon CodeCatalyst

Acciones definidas por Amazon CodeCatalyst

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptConnection [solo permiso]	Concede permiso para aceptar una solicitud para conectar esta cuenta a un CodeCatalyst espacio de Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateIamRoleToConnection [solo permiso]	Concede permiso para asociar un rol de IAM a una conexión	Escritura	connections*		iam:PassRole
				aws:ResourceTag/${TagKey}	
AssociateIdentityCenterApplicationToSpace [solo permiso]	Otorga permiso para asociar una aplicación del Centro de Identidad de IAM a un espacio de Amazon CodeCatalyst	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
AssociateIdentityToIdentity	Otorga permiso para asociar una identidad a una aplicación del Centro de Identidad	Escritura	identity-center-ap		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CenterApplication [solo permiso]	de IAM para un espacio de Amazon CodeCatalyst		plications*		
				aws:ResourceTag/${TagKey}	
BatchAssociateIdentitiesToIdentityCenterApplication [solo permiso]	Otorga permiso para asociar varias identidades a una aplicación del Centro de Identidad de IAM para un espacio de Amazon CodeCatalyst	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateIdentitiesFromIdentityCenterApplication [solo permiso]	Otorga permiso para desasociar varias identidades de una aplicación del Centro de Identidad de IAM para un espacio de Amazon CodeCatalyst	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
CreateIdentityCenterApplication [solo permiso]	Otorga permiso para crear una aplicación del IAM Identity Center	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSpace [solo permiso]	Otorga permiso para crear un CodeCatalyst espacio en Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSpaceAdminRoleAssignment [solo permiso]	Otorga permiso para crear una asignación de funciones de administrador para un CodeCatalyst espacio de Amazon y una aplicación de IAM Identity Center determinados	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DeleteConnection [solo permiso]	Concede permiso para eliminar una conexión.	Escritura	connections*		
				aws:ResourceTag/${TagKey}	
DeleteIdentityCenterApplication [solo permiso]	Otorga permiso para eliminar la aplicación del IAM Identity Center	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateIamRoleFromConnection [solo permiso]	Concede permiso para desasociar un rol de IAM de una conexión	Escritura	connections*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityCenterApplicationFromSpace [solo permiso]	Concede permiso para desasociar una aplicación del Centro de Identidad de IAM de un espacio de Amazon CodeCatalyst	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityFromIdentityCenterApplication [solo permiso]	Concede permiso para desasociar una identidad de una aplicación del Centro de Identidad de IAM para un espacio de Amazon CodeCatalyst	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetBillingAuthorization [solo permiso]	Concede permiso para describir la autorización de facturación de una conexión	Lectura	connections*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnection [solo permiso]	Concede permiso para obtener una conexión	Lectura	connections*		
				aws:ResourceTag/${TagKey}	
GetIdentityCenterApplication [solo permiso]	Otorga permiso para obtener más información sobre una aplicación del IAM Identity Center	Lectura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetPendingConnection [solo permiso]	Concede permiso para obtener una solicitud pendiente para conectar esta cuenta a un CodeCatalyst espacio de Amazon	Lectura			
ListConnections [solo permiso]	Concede permiso para enumerar las conexiones que no están pendientes	Enumeración			
ListIamRolesForConnection [solo permiso]	Concede permiso para enumerar los roles de IAM asociados a una conexión	Enumeración	connections*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIdentityCenterApplications [solo permiso]	Otorga permiso para ver una lista de todas las aplicaciones del IAM Identity Center de la cuenta	Enumeración			
ListIdentityCenterApplicationsForSpace [solo permiso]	Concede permiso para ver una lista de aplicaciones del IAM Identity Center por Amazon space CodeCatalyst	Enumeración			
ListSpacesForIdentityCenterApplication [solo permiso]	Otorga permiso para ver una lista de CodeCatalyst espacios de Amazon mediante la aplicación IAM Identity Center	Enumeración	identity-center-application*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [solo permiso]	Otorga permiso para enumerar etiquetas para un CodeCatalyst recurso de Amazon	Lectura	connections		
			identity-center-applications		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutBillingAuthorization [solo permiso]	Concede permiso para crear o actualizar la autorización de facturación de una conexión	Escritura	connections*		
				aws:ResourceTag/${TagKey}	
RejectConnection [solo permiso]	Concede permiso para rechazar una solicitud de conexión de esta cuenta a un CodeCatalyst espacio de Amazon	Escritura			
SynchronizeIdentityCenterApplication [solo permiso]	Otorga permiso para sincronizar una aplicación del IAM Identity Center con el almacén de identidades de respaldo	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
TagResource [solo permiso]	Otorga permiso para etiquetar un CodeCatalyst recurso de Amazon	Etiquetado	connections		
			identity-center-applications		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [solo permiso]	Otorga permiso para desetiquetar un recurso de Amazon CodeCatalyst	Etiquetado	connections		
			identity-center-applications		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateIdentityCenterApplication [solo permiso]	Otorga permiso para actualizar una aplicación a IAM Identity Center	Escritura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon CodeCatalyst

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
connections	`arn:${Partition}:codecatalyst:${Region}:${Account}:/connections/${ConnectionId}`	aws:ResourceTag/${TagKey}
identity-center-applications	`arn:${Partition}:codecatalyst:${Region}:${Account}:/identity-center-applications/${IdentityCenterApplicationId}`	aws:ResourceTag/${TagKey}
space	`arn:${Partition}:codecatalyst:::space/${SpaceId}`	
project	`arn:${Partition}:codecatalyst:::space/${SpaceId}/project/${ProjectId}`	

Claves de estado de Amazon CodeCatalyst

Amazon CodeCatalyst define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS CodeCommit

AWS CodeCommit (prefijo de servicio:`codecommit`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodeCommit
- Tipos de recursos definidos por AWS CodeCommit
- Claves de condición de AWS CodeCommit

Acciones definidas por AWS CodeCommit

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateApprovalRuleTemplateWithRepository	Concede permiso para asociar una plantilla de regla de aprobación a un repositorio	Write	repository*		
BatchAssociateApprovalRuleTemplateWithRepositories	Concede permiso para asociar una plantilla de regla de aprobación con varios repositorios en una sola operación	Write	repository*		
BatchDescribeMergeConflicts	Da permiso para obtener información acerca de varias conflictos de combinación al intentar combinar dos confirmaciones mediante una combinación de tres modos o la opción de combinación de squash.	Read	repository*		
BatchDisassociateApprovalRuleTemplateFromRepositories	Concede permiso para quitar la asociación entre una plantilla de regla de aprobación y varios repositorios en una sola operación	Escritura	repository*		
BatchGetCommits	Otorga permiso para devolver información sobre una o más	Lectura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	confirmaciones de un repositorio AWS CodeCommit				
BatchGetPullRequests [solo permiso]	Otorga permiso para devolver información sobre una o más solicitudes de incorporación de cambios en un AWS CodeCommit repositorio	Lectura	repository*		
BatchGetRepositories	Da permiso para obtener información sobre varios repositorios.	Read	repository*		
CancelUploadArchive [solo permiso]	Otorga permiso para cancelar la carga de un archivo a una canalización en AWS CodePipeline	Lectura	repository*		
CreateApprovalRuleTemplate	Concede permiso para crear una plantilla de regla de aprobación que creará automáticamente reglas de aprobación en solicitudes de extracción que coincidan con las condiciones definidas en la plantilla; no concede permisos para crear reglas de aprobación para solicitudes de extracción individuales	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBranch	Otorga permiso para crear una rama en un AWS CodeCommit repositorio con esta API; no controla las acciones de creación de sucursales de Git	Escritura	repository*		
				codecommit:References	
CreateCommit	Otorga permiso para añadir, copiar, mover o actualizar uno o varios archivos de una rama de un AWS CodeCommit repositorio y generar una confirmación de los cambios en la rama especificada	Escritura	repository*		
				codecommit:References	
CreatePullRequest	Da permiso para crear una solicitud de extracción en el repositorio especificado.	Write	repository*		
CreatePullRequestApprovalRule	Concede permiso para crear una regla de aprobación específica para una solicitud de extracción individual; no concede permisos para crear plantillas de regla de aprobación	Escritura	repository*		
CreateRepository	Otorga permiso para crear un AWS CodeCommit repositorio	Escritura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUnreferencedMergeCommit	Da permiso para crear una confirmación sin referencia que contiene el resultado de combinar dos confirmaciones realizadas mediante la opción de combinación de tres modos o de squash; no controla las acciones de combinación de Git.	Write	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	Concede permiso para eliminar una plantilla de regla de aprobación	Escritura			
DeleteBranch	Otorga permiso para eliminar una rama en un AWS CodeCommit repositorio con esta API; no controla las acciones de eliminación de ramas de Git	Escritura	repository*		
				codecommit:References	
DeleteCommentContent	Da permiso para eliminar el contenido de un comentario realizado en un cambio, archivo o confirmación en un repositorio.	Write	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFile	Da permiso para eliminar un archivo especificado de una ramificación especificada.	Write	repository*		
				codecommit:References	
DeletePullRequestApprovalRule	Concede permiso para eliminar la regla de aprobación creada para una solicitud de extracción si la regla no fue creada por una plantilla de regla de aprobación	Escritura	repository*		
DeleteRepository	Otorga permiso para eliminar un AWS CodeCommit repositorio	Escritura	repository*		
DescribeMergeConflicts	Da permiso para obtener información acerca de conflictos de combinación específicos al intentar combinar dos confirmaciones mediante una opción de combinación de tres modos o de squash.	Read	repository*		
DescribePullRequestEvents	Da permiso para devolver información sobre uno o varios eventos de solicitud de extracción.	Read	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateApprovalRuleTemplateFromRepository	Concede permiso para quitar la asociación entre una plantilla de regla de aprobación y un repositorio	Write	repository*		
EvaluatePullRequestApprovalRules	Concede permiso para evaluar si una solicitud de extracción es combinable según su estado de aprobación actual y los requisitos de la regla de aprobación	Read	repository*		
GetApprovalRuleTemplate	Concede permiso para devolver la información sobre una plantilla de regla de aprobación	Lectura			
GetBlob	Otorga permiso para ver el contenido codificado de un archivo individual de un AWS CodeCommit repositorio desde la AWS CodeCommit consola	Lectura	repository*		
GetBranch	Otorga permiso para obtener detalles sobre una rama en un AWS CodeCommit repositorio con esta API; no controla las acciones de la rama de Git	Lectura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetComment	Da permiso para obtener el contenido de un comentario realizado en un cambio, archivo o confirmación de un repositorio.	Read	repository*		
GetCommentReactions	Concede permiso para obtener las reacciones en un comentario	Read	repository*		
GetCommentsForComparedCommit	Da permiso para obtener información sobre los comentarios realizados en la comparación entre dos confirmaciones.	Read	repository*		
GetCommentsForPullRequest	Da permiso para obtener comentarios realizados en una solicitud de extracción.	Read	repository*		
GetCommit	Da permiso para devolver información sobre una confirmación, incluidos el mensaje de confirmación y la información del confirmador, con esta API; no controla acciones de registro de Git.	Read	repository*		
GetCommitHistory [solo permiso]	Da permiso para obtener información sobre el historial de confirmaciones de un repositorio.	Read	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCommitsFromMergeBase [solo permiso]	Da permiso para obtener información sobre la diferencia entre confirmaciones en el contexto de una posible combinación.	Read	repository*		
GetDifferences	Da permiso para ver información sobre las diferencias entre especificadores de confirmación válidos, como, por ejemplo, una ramificación, una etiqueta, HEAD, el ID de confirmación u otra referencia completa.	Read	repository*		
GetFile	Da permiso para devolver el contenido codificado en base-64 de un archivo especificado y sus metadatos.	Read	repository*		
GetFolder	Da permiso para devolver el contenido de una carpeta especificada en un repositorio.	Read	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMergeCommit	Da permiso para obtener información acerca de una confirmación de combinación creada mediante una de las opciones de combinación para las solicitudes de extracción que crean las confirmaciones de combinación. No todas las opciones de combinación crean confirmaciones de combinación. Este permiso no controla las acciones de combinación de Git.	Lectura	repository*		
				codecommit:References	
GetMergeConflicts	Otorga permiso para obtener información sobre los conflictos de fusión entre la confirmación anterior y posterior IDs de una solicitud de extracción en un repositorio	Lectura	repository*		
GetMergeOptions	Da permiso para obtener información acerca de las opciones de combinación para solicitudes de extracción que se pueden utilizar para combinar dos confirmaciones; no controla las acciones de combinación de Git.	Read	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetObjectIdentifier [solo permiso]	Da permisos para resolver blobs, árboles y confirmaciones con su identificador.	Read	repository*		
GetPullRequest	Da permiso para obtener información acerca de una solicitud de extracción de un repositorio especificado.	Read	repository*		
GetPullRequestApprovalStates	Concede permiso para recuperar las aprobaciones actuales en una solicitud de extracción introducida	Read	repository*		
GetPullRequestOverrideState	Concede permiso para recuperar el estado de anulación actual de una solicitud de extracción dada	Read	repository*		
GetReferences [solo permiso]	Otorga permiso para obtener detalles sobre las referencias de un AWS CodeCommit repositorio; no controla las acciones de referencia de Git	Lectura	repository*		
GetRepository	Otorga permiso para obtener información sobre un AWS CodeCommit repositorio	Lectura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRepositoryTriggers	Da permiso para obtener información acerca de desencadenadores configurados para un repositorio.	Read	repository*		
GetTree [solo permiso]	Otorga permiso para ver el contenido de un árbol específico en un AWS CodeCommit repositorio desde la AWS CodeCommit consola	Lectura	repository*		
GetUploadArchiveStatus [solo permiso]	Otorga permiso para obtener información sobre el estado de un archivo subido a una canalización en AWS CodePipeline	Lectura	repository*		
GitPull [solo permiso]	Otorga permiso para extraer información de un AWS CodeCommit repositorio a un repositorio local	Lectura	repository*		
GitPush [solo permiso]	Otorga permiso para enviar información de un repositorio local a un repositorio AWS CodeCommit	Escritura	repository*		
				codecommit:References	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApprovalRuleTemplates	Otorga permiso para enumerar todas las plantillas de reglas de aprobación en una Región de AWS para Cuenta de AWS	Enumeración			
ListAssociatedApprovalRuleTemplatesForRepository	Concede permiso para enumerar las plantillas de reglas de aprobación asociadas a un repositorio	Enumeración	repository*		
ListBranches	Otorga permiso para enumerar las ramas de un AWS CodeCommit repositorio con esta API; no controla las acciones de las ramas de Git	Enumeración	repository*		
ListFileCommitHistory	Concede permiso para enumerar las confirmaciones y los cambios en un archivo especificado	Enumeración	repository*		
ListPullRequests	Da permiso para generar una lista de solicitudes de extracción de un repositorio especificado.	Enumeración	repository*		
ListRepositories	Otorga permiso para incluir información sobre AWS CodeCommit los repositorios de la región actual para su Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRepositoriesForApprovalRuleTemplate	Concede permiso para mostrar los repositorios asociados a una plantilla de regla de aprobación	Enumeración			
ListTagsForResource	Otorga permiso para incluir el recurso adjunto a un ARN CodeCommit de recurso	Enumeración	repository		
MergeBranchesByFastForward	Da permiso para combinar dos confirmaciones en la ramificación de destino especificada mediante la opción de combinación de avance rápido.	Write	repository*		
				codecommit:References	
MergeBranchesBySquash	Da permiso para combinar dos confirmaciones en la ramificación de destino especificada mediante la opción de combinación de squash.	Write	repository*		
				codecommit:References	
MergeBranchesByThreeWay	Da permiso para combinar dos confirmaciones en la ramificación de destino especificada mediante la opción de combinación de tres modos.	Write	repository*		
				codecommit:References	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
MergePullRequestByFastForward	Da permiso para cerrar una solicitud de extracción e intentar combinarla en la ramificación de destino especificada para dicha solicitud de extracción en la confirmación especificada mediante la opción de combinación de avance rápido.	Write	repository*		
				codecommit:References	
MergePullRequestBySquash	Da permiso para cerrar una solicitud de extracción e intentar combinarla en la ramificación de destino especificada para dicha solicitud de extracción en la confirmación especificada mediante la opción de combinación de squash.	Write	repository*		
				codecommit:References	
MergePullRequestByThreeWay	Da permiso para cerrar una solicitud de extracción e intentar combinarla en la ramificación de destino especificada para dicha solicitud de extracción en la confirmación especificada mediante la opción de combinación de tres modos.	Write	repository*		
				codecommit:References	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
OverridePullRequestApprovalRules	Concede permiso para anular todas las reglas de aprobación de una solicitud de extracción, incluidas las reglas de aprobación creadas por una plantilla	Write	repository*		
PostCommentForComparedCommit	Da permiso para publicar un comentario en la comparación entre dos confirmaciones.	Write	repository*		
PostCommentForPullRequest	Da permiso para publicar un comentario en una solicitud de extracción.	Write	repository*		
PostCommentReply	Da permiso para publicar un comentario en respuesta a un comentario existente en una comparación entre confirmaciones o en una solicitud de extracción.	Write	repository*		
PutCommentReaction	Concede permiso para publicar una reacción en un comentario	Escritura	repository*		
PutFile	Otorga permiso para añadir o actualizar un archivo en una rama de un AWS CodeCommit repositorio y generar una confirmación para añadirlo en la rama especificada	Escritura	repository*		
				codecommit:References	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutRepositoryTriggers	Da permiso para crear, actualizar o eliminar desencadenadores para un repositorio.	Escritura	repository*		
TagResource	Otorga permiso para adjuntar etiquetas de recursos a un CodeCommit ARN de recurso	Etiquetado	repository		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TestRepositoryTriggers	Da permiso para probar la funcionalidad de los desencadenadores de repositorio enviando información al objetivo del desencadenador.	Escritura	repository*		
UntagResource	Otorga permiso para desasociar etiquetas de recursos de un ARN de CodeCommit recurso	Etiquetado	repository		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApprovalRuleTemplateContent	Concede permiso para actualizar el contenido de las plantillas de las reglas de aprobación; no concede permisos para actualizar el contenido de las reglas de aprobación creadas específicamente para las solicitudes de extracción	Write			
UpdateApprovalRuleTemplateDescription	Concede permiso para actualizar la descripción de las plantillas de las reglas de aprobación	Write			
UpdateApprovalRuleTemplateName	Concede permiso para actualizar el nombre de las plantillas de las reglas de aprobación	Write			
UpdateComment	Da permiso para actualizar el contenido de un comentario si la identidad coincide con la identidad que se utiliza para crear el comentario.	Escritura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDefaultBranch	Otorga permiso para cambiar la rama predeterminada de un repositorio AWS CodeCommit	Escritura	repository*		
UpdatePullRequestApprovalRuleContent	Concede permiso para actualizar el contenido para reglas de aprobación creadas para solicitudes de extracción específicas; no concede permisos para actualizar el contenido de las reglas de aprobación para reglas creadas con una plantilla de reglas de aprobación	Write	repository*		
UpdatePullRequestApprovalState	Concede permiso para actualizar el estado de aprobación de las solicitudes de extracción	Write	repository*		
UpdatePullRequestDescription	Da permiso para actualizar la descripción de una solicitud de extracción.	Write	repository*		
UpdatePullRequestStatus	Da permiso para actualizar el estado de una solicitud de extracción.	Write	repository*		
UpdatePullRequestTitle	Da permiso para actualizar el título de una solicitud de extracción.	Escritura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRepositoryDescription	Otorga permiso para cambiar la descripción de un AWS CodeCommit repositorio	Escritura	repository*		
UpdateRepositoryEncryptionKey	Otorga permiso para cambiar la clave de cifrado de AWS KMS utilizada para cifrar y descifrar un repositorio AWS CodeCommit	Escritura	repository*		
UpdateRepositoryName	Otorga permiso para cambiar el nombre de un repositorio AWS CodeCommit	Escritura	repository*		
UploadArchive [solo permiso]	Otorga permiso al rol de servicio AWS CodePipeline para cargar los cambios del repositorio en una canalización	Escritura	repository*		

Tipos de recursos definidos por AWS CodeCommit

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
repository	`arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS CodeCommit

AWS CodeCommit define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
codecommit:References	Filtra el acceso por referencia de Git a AWS CodeCommit acciones específicas	Cadena

Acciones, recursos y claves de condición para AWS CodeConnections

AWS CodeConnections (prefijo de servicio:`codeconnections`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodeConnections
- Tipos de recursos definidos por AWS CodeConnections
- Claves de condición de AWS CodeConnections

Acciones definidas por AWS CodeConnections

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnection	Concede permiso para crear un recurso Connection	Write		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateHost	Concede permiso para crear un recurso de host	Escritura		aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys codeconnections:ProviderType codeconnections:VpcId	
CreateRepositoryLink	Otorga permiso para crear un enlace de repositorio	Escritura	Connection*		codeconnections:PassConnection codeconnections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSyncConfiguration	Otorga permiso para crear una configuración de plantilla sincronizada	Escritura	RepositoryLink*		codeconnections:PassRepository iam:PassRole
				codeconnections:Branch	
DeleteConnection	Concede permiso para eliminar un recurso Connection	Write	Connection*		
DeleteHost	Concede permiso para eliminar un recurso de host	Escritura	Host*		
DeleteRepositoryLink	Otorga permiso para eliminar un enlace de repositorio	Escritura	RepositoryLink*		
DeleteSyncConfiguration	Otorga permiso para eliminar una configuración de sincronización	Escritura			
GetConnection	Concede permiso para obtener detalles sobre un recurso Connection	Lectura	Connection*		
GetConnectionToken [solo permiso]	Concede permiso para obtener un token de conexión para llamar a las acciones del proveedor	Lectura	Connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetHost	Concede permiso para obtener información detallada acerca de un recurso de host	Read	Host*		
GetIndividualAccessToken [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Read		codeconnections:ProviderType	codeconnections:StartOAuthHandshake
GetInstallationUrl [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Lectura		codeconnections:ProviderType	
GetRepositoryLink	Otorga permiso para describir un enlace de repositorio	Lectura	RepositoryLink*		
GetRepositorySyncStatus	Otorga permiso para obtener el estado de sincronización más reciente de un repositorio	Lectura	RepositoryLink*		
				codeconnections:Branch	
GetResourceSyncStatus	Concede permiso para obtener el estado de sincronización más reciente de un recurso (pila cfn u otros recursos)	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSyncBlockerSummary	Concede permiso para describir los bloqueadores de sincronización de servicio en un recurso (pila cfn u otros recursos)	Lectura			
GetSyncConfiguration	Concede permiso para describir una configuración de sincronización	Lectura			
ListConnections	Concede permiso para enumerar los recursos Connection	List	Connection*		
				codeconnections:ProviderTypeFilter	
ListHosts	Concede permiso para mostrar los recursos de host	List		codeconnections:ProviderTypeFilter	
ListInstallationTargets [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Enumeración			codeconnections:GetIndividualAccessToken codeconnections:StartOAuthHandshake

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRepositoryLinks	Otorga permiso para enumerar enlaces de repositorios	Enumeración			
ListRepositorySyncDefinitions	Otorga permiso para enumerar definiciones de sincronización de repositorios	Enumeración			
ListSyncConfigurations	Concede permiso para mostrar una lista de las configuraciones de sincronización para un enlace de repositorio	Enumeración			
ListTagsForResource	Concede permiso al conjunto de pares de clave-valor que se utiliza para administrar el recurso	Enumeración	Connection		
			Host		
			RepositoryLink		
PassConnection [solo permiso]	Otorga permiso para pasar un recurso de conexión a un AWS servicio que acepta un ARN de conexión como entrada, como codepipeline: CreatePipeline	Lectura	Connection*		
				codeconnections:PassedToService	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PassRepository [solo permiso]	Otorga permiso para pasar un recurso de enlace de repositorio a un AWS servicio que acepta un RepositoryLinkId como entrada, como codeconnections: CreateSyncConfiguration	Lectura	RepositoryLink*		
				codeconnections:PassedToService	
RegisterAppCode [solo permiso]	Otorga permiso para asociar un servidor de terceros, como una instancia de GitHub Enterprise Server, a un host	Lectura		codeconnections:HostArn	
StartAppRegistrationHandshake [solo permiso]	Otorga permiso para asociar un servidor de terceros, como una instancia de GitHub Enterprise Server, a un host	Lectura		codeconnections:HostArn	
StartOAuthHandshake [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Lectura		codeconnections:ProviderType	
TagResource	Concede permiso para agregar o modificar las etiquetas del recurso especificado.	Etiquetado	Connection		
			Host		
			RepositoryLink		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un AWS recurso	Etiquetado	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnectionInstallation	Otorga permiso para actualizar un recurso de Connection con una instalación de la aplicación CodeStar Connections	Escritura	Connection*		codeconnections:GetIndividualAccessToken codeconnections:GetInstallationUrl codeconnections:ListInstallationTargets codeconnections:StartOAuthHandshake
				codeconnections:InstallationId	
UpdateHost	Concede permiso para actualizar un recurso de host.	Escritura	Host*		
				codeconnections:VpcId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRepositoryLink	Otorga permiso para actualizar un enlace de repositorio	Escritura	RepositoryLink*		
UpdateSyncBlocker	Otorga permiso para actualizar un bloqueador de sincronización para un recurso (pila cfn u otros recursos)	Escritura			
UpdateSyncConfiguration	Otorga permiso para actualizar una configuración de sincronización	Escritura		codeconnections:Branch	
UseConnection [solo permiso]	Concede permiso para usar un recurso Connection para llamar a acciones del proveedor	Lectura	Connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				codeconnections:BranchName codeconnections:FullRepositoryId codeconnections:OwnerId codeconnections:ProviderAction codeconnections:ProviderPermissionsRequired codeconnections:RepositoryName	

Tipos de recursos definidos por AWS CodeConnections

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Connection	`arn:${Partition}:codeconnections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codeconnections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codeconnections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS CodeConnections

AWS CodeConnections define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
codeconnections:Branch	Filtra el acceso por el nombre de ramificación que se incluye en la solicitud	Cadena
codeconnections:BranchName	Filtra el acceso por el nombre de ramificación que se incluye en la solicitud. Se aplica solo a UseConnection las solicitudes de acceso a una rama de repositorio específica	Cadena
codeconnections:FullRepositoryId	Filtra el acceso del repositorio que se incluye en la solicitud. Se aplica solo a UseConnection las solicitudes de acceso a un repositorio específico	Cadena
codeconnections:HostArn	Filtra el acceso por el recurso de host asociado a la conexión utilizada en la solicitud	ARN
codeconnections:InstallationId	Filtra el acceso por el ID de terceros (como el ID de instalación de la aplicación Bitbucket CodeConnections) que se utiliza para actualizar una conexión. Le permite restringir las instalaciones de aplicaciones de terceros que se pueden utilizar para realizar una Connection	Cadena
codeconnections:OwnerId	Filtra el acceso por propietario del repositorio de terceros. Se aplica solo a UseConnection las solicitudes de acceso a los repositorios propiedad de un usuario específico	Cadena
codeconnections:PassedToService	Filtra el acceso por el servicio al que el principal puede transferir una conexión o RepositoryLink	Cadena

Claves de condición	Descripción	Tipo
codeconnections:ProviderAction	Filtra el acceso por la acción del proveedor en una UseConnection solicitud como ListRepositories. Consulte la documentación para ver todos los valores válidos	Cadena
codeconnections:ProviderPermissionsRequired	Filtra el acceso mediante los permisos de escritura de una acción del proveedor en una UseConnection solicitud . Los tipos válidos son read_only y read_write	Cadena
codeconnections:ProviderType	Filtra el acceso por el tipo de proveedor externo incluido en la solicitud	Cadena
codeconnections:ProviderTypeFilter	Filtra el acceso por el tipo de proveedor externo utilizado para filtrar resultados	Cadena
codeconnections:RepositoryName	Filtra el acceso por el nombre del repositorio que se incluye en la solicitud. Solo se aplica a UseConnection las solicitudes de acceso a los repositorios propiedad de un usuario específico	Cadena
codeconnections:VpcId	Filtra el acceso según lo VpcId aprobado en la solicitud	Cadena

Acciones, recursos y claves de condición para AWS CodeDeploy

AWS CodeDeploy (prefijo de servicio:`codedeploy`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodeDeploy
- Tipos de recursos definidos por AWS CodeDeploy
- Claves de condición de AWS CodeDeploy

Acciones definidas por AWS CodeDeploy

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTagsToOnPremisesInstances	Concede permiso para añadir etiquetas a una o varias instancias en las instalaciones	Etiquetado	instance*		
BatchGetApplicationRevisions	Concede permiso para obtener información sobre una o varias revisiones de aplicaciones	Lectura	application*		
BatchGetApplications	Concede permiso para obtener información sobre varias aplicaciones asociadas al usuario de IAM	Lectura	application*		
BatchGetDeploymentGroups	Concede permiso para obtener información sobre uno o varios grupos de implementación	Lectura	deploymentgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetDeploymentInstances	Concede permiso para obtener información sobre una o varias instancias que forman parte de un grupo de implementaciones	Lectura	deploymentgroup*		
BatchGetDeploymentTargets	Concede permiso para devolver una matriz de uno o varios destinos asociados a una implementación. Este método funciona con todos los tipos de procesamiento y debe usarse en lugar del obsoleto BatchGetDeploymentInstances. El número máximo de destinos que se puede devolver es 25	Lectura			
BatchGetDeployments	Concede permiso para obtener información sobre varias implementaciones asociadas al usuario de IAM	Lectura	deploymentgroup*		
BatchGetOnPremisesInstances	Concede permiso para obtener información sobre una o varias instancias en las instalaciones	Lectura	instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ContinueDeployment	Concede permiso para iniciar el proceso de redirigir el tráfico de instancias en el entorno original a instancias en el entorno de sustitución sin tener que esperar a que transcurra un tiempo de espera especificado	Escritura			
CreateApplication	Concede permiso para crear una aplicación asociada al usuario de IAM	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [solo permiso]	Otorga permiso para crear un CloudFormation despliegue que coopere con la orquestación de una actualización de la pila CloudFormation	Escritura			
CreateDeployment	Concede permiso para crear una implementación para una aplicación asociada al usuario de IAM	Escritura	deploymentgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeploymentConfig	Concede permiso para crear una configuración de implementación personalizada asociada al usuario de IAM	Escritura	deploymentconfig*		
CreateDeploymentGroup	Concede permiso para crear un grupo de implementación para una aplicación asociada al usuario de IAM	Escritura	deploymentgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permiso para eliminar una aplicación asociada al usuario de IAM	Escritura	application*		
DeleteDeploymentConfig	Concede permiso para eliminar una configuración de implementación personalizada asociada al usuario de IAM	Escritura	deploymentconfig*		
DeleteDeploymentGroup	Concede permiso para eliminar un grupo de implementación para una aplicación asociada al usuario de IAM	Escritura	deploymentgroup*		
DeleteGitHubAccountToken	Otorga permiso para eliminar la conexión de una cuenta GitHub	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcesByExternalId	Concede permiso para eliminar los recursos asociados con el ID externo especificado	Escritura			
DeregisterOnPremisesInstance	Concede permiso para cancelar el registro de una instancia en las instalaciones	Escritura	instance*		
GetApplication	Concede permiso para obtener información sobre una sola aplicación asociada al usuario de IAM	Enumeración	application*		
GetApplicationRevision	Concede permiso para obtener información sobre una sola revisión de aplicación para una aplicación asociada al usuario de IAM	Enumeración	application*		
GetDeployment	Concede permiso para obtener información sobre una sola implementación de un grupo de implementaciones para una aplicación asociada al usuario de IAM	Enumeración	deploymentgroup*		
GetDeploymentConfig	Concede permiso para obtener información sobre una sola configuración de implementación asociada al usuario de IAM	Enumeración	deploymentconfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeploymentGroup	Concede permiso para obtener información sobre un solo grupo de implementaciones para una aplicación asociada al usuario de IAM	Enumeración	deploymentgroup*		
GetDeploymentInstance	Concede permiso para obtener información sobre una sola instancia de una implementación asociada al usuario de IAM	Enumeración	deploymentgroup*		
GetDeploymentTarget	Concede permiso para devolver información acerca de un destino de la implementación	Lectura			
GetOnPremisesInstance	Concede permiso para obtener información sobre una sola instancia en las instalaciones	Enumeración	instance*		
ListApplicationRevisions	Concede permiso para obtener información sobre todas las revisiones de aplicación para una aplicación asociada al usuario de IAM	Enumeración	application*		
ListApplications	Concede permiso para obtener información sobre todas las aplicaciones asociadas al usuario de IAM	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeploymentConfigs	Concede permiso para obtener información sobre todas las configuraciones de implementación asociadas al usuario de IAM	Enumeración			
ListDeploymentGroups	Concede permiso para obtener información sobre todos los grupos de implementación para una aplicación asociada al usuario de IAM	Enumeración	application*		
ListDeploymentInstances	Concede permiso para obtener información sobre todas las instancias de una implementación asociada al usuario de IAM	Enumeración	deploymentgroup*		
ListDeploymentTargets	Otorga permiso para devolver una matriz de objetivos IDs asociados a una implementación	Enumeración			
ListDeployments	Concede permiso para obtener información sobre todas las implementaciones de un grupo de implementaciones asociado al usuario de IAM, o para obtener todas las implementaciones asociadas al usuario de IAM	Enumeración	deploymentgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGitHubAccountTokenNames	Otorga permiso para enumerar los nombres de las conexiones almacenadas a GitHub las cuentas	Enumeración			
ListOnPremisesInstances	Concede permiso para obtener una lista de uno o varios nombres de instancias en las instalaciones	Enumeración			
ListTagsForResource	Concede permiso para devolver una lista de etiquetas para el recurso identificado por un ARN especificado. Las etiquetas se utilizan para organizar y clasificar los recursos CodeDeploy	Enumeración	application deploymentgroup		
PutLifecycleEventHookExecutionStatus	Concede permiso para notificar un estado de ejecución de un enlace de evento de ciclo de vida para la implementación asociada al usuario de IAM	Escritura			
RegisterApplicationRevision	Concede permiso para registrar información acerca de una revisión de aplicación para una aplicación asociada al usuario de IAM	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterOnPremisesInstance	Concede permiso para registrar una instancia en las instalaciones	Escritura	instance*		
RemoveTagsFromOnPremisesInstances	Concede permiso para eliminar etiquetas de una o varias instancias en las instalaciones	Etiquetado	instance*		
SkipWaitTimeForInstanceTermination	Concede permiso para anular cualquier tiempo de espera especificado y comienza a terminar las instancias inmediatamente después de completar el enrutamiento del tráfico. Esta acción se aplica únicamente a las implementaciones azul/verde	Escritura			
StopDeployment	Concede permiso para detener una implementación	Escritura			
TagResource	Otorga permiso para asociar la lista de etiquetas del parámetro Etiquetas de entrada con el recurso identificado por el parámetro ResourceArn de entrada	Etiquetado	application		
			deploymentgroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para desasociar un recurso de una lista de etiquetas. El recurso se identifica mediante el parámetro ResourceArn de entrada. Las etiquetas se identifican mediante la lista de claves del parámetro de TagKeys entrada	Etiquetado	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	application*		
UpdateDeploymentGroup	Concede permiso para cambiar información sobre un solo grupo de implementaciones para una aplicación asociada al usuario de IAM	Escritura	deploymentgroup*		

Tipos de recursos definidos por AWS CodeDeploy

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}`	aws:ResourceTag/${TagKey}
deploymentconfig	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}`	
deploymentgroup	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}`	aws:ResourceTag/${TagKey}
instance	`arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}`	

Claves de condición de AWS CodeDeploy

AWS CodeDeploy define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Claves de condición, recursos y acciones para el servicio de comandos de host AWS CodeDeploy seguro

AWS CodeDeploy El servicio secure host commands (prefijo de servicio:`codedeploy-commands-secure`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodeDeploy el servicio de comandos secure host
- Tipos de recursos definidos por el servicio de comandos AWS CodeDeploy Secure Host
- Claves de condición para AWS CodeDeploy un servicio seguro de comandos de host

Acciones definidas por AWS CodeDeploy el servicio de comandos secure host

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeploymentSpecification	Otorga permiso para obtener una especificación de implementación	Lectura			
PollHostCommand	Otorga permiso para solicitar comandos del agente de host	Lectura			
PutHostCommandAcknowledgement	Otorga permiso para marcar los comandos del agente de host confirmados	Escritura			
PutHostCommandComplete	Otorga permiso para marcar los comandos del agente de host completados	Escritura			

Tipos de recursos definidos por el servicio de comandos AWS CodeDeploy Secure Host

AWS CodeDeploy el servicio secure host commands no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al servicio AWS CodeDeploy seguro de comandos de host, especifíquelo `"Resource": "*"` en su política.

Claves de condición para AWS CodeDeploy un servicio seguro de comandos de host

CodeDeploy Commands Secure no tiene claves de contexto específicas del servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de Amazon CodeGuru

Amazon CodeGuru (prefijo de servicio:`codeguru`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CodeGuru
- Tipos de recursos definidos por Amazon CodeGuru
- Claves de estado de Amazon CodeGuru

Acciones definidas por Amazon CodeGuru

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCodeGuruFreeTrialSummary [solo permiso]	Otorga permiso para obtener un resumen de la versión de prueba gratuita del CodeGuru servicio, que incluye la fecha de caducidad	Lectura			

Tipos de recursos definidos por Amazon CodeGuru

Amazon CodeGuru no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a Amazon CodeGuru, `"Resource": "*"` especifícalo en tu política.

Claves de estado de Amazon CodeGuru

CodeGuru no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones de Amazon CodeGuru Profiler

Amazon CodeGuru Profiler (prefijo de servicio:`codeguru-profiler`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CodeGuru Profiler
- Tipos de recursos definidos por Amazon CodeGuru Profiler
- Claves de condición de Amazon CodeGuru Profiler

Acciones definidas por Amazon CodeGuru Profiler

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddNotificationChannels	Otorga permiso para añadir hasta dos temas ARNs de los temas de AWS SNS existentes para publicar notificaciones	Escritura	ProfilingGroup*		
BatchGetFrameMetricData	Concede permiso para obtener los datos de métrica de trama para un grupo de creación de perfiles	Enumeración	ProfilingGroup*		
ConfigureAgent	Otorga permiso para registrarse en el servicio de orquestación y recuperar información de configuración de perfiles que utilizan los agentes	Escritura	ProfilingGroup*		
CreateProfilingGroup	Concede permiso para crear un grupo de perfiles	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteProfilingGroup	Concede permiso para eliminar un grupo de perfiles	Write	ProfilingGroup*		
DescribeProfilingGroup	Concede permiso para describir un grupo de perfiles	Read	ProfilingGroup*		
GetFindingsReportAccountSummary	Concede permiso para obtener un resumen de las recomendaciones recientes	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	para cada grupo de perfiles de la cuenta				
GetNotificationConfiguration	Concede permiso para obtener la configuración de notificación	Lectura	Profiling Group*		
GetPolicy	Concede permiso para obtener la política de recursos asociada al grupo de creación de perfiles especificado	Lectura	Profiling Group*		
GetProfile	Concede permiso para obtener perfiles agregados para un grupo de perfiles específico	Read	Profiling Group*		
GetRecommendations	Concede permiso para obtener recomendaciones	Read	Profiling Group*		
ListFindingsReports	Concede permiso para enumerar los informes de recomendaciones disponibles para un grupo de perfiles específico	List	Profiling Group*		
ListProfileTimes	Concede permiso para enumerar los tiempos de inicio de los perfiles agregados disponibles para un grupo de perfiles específico	List	Profiling Group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProfilingGroups	Concede permiso para enumerar grupos de perfiles en la cuenta	List			
ListTagsForResource	Concede permiso para enumerar etiquetas para un grupo de creación de perfiles	Enumeración	Profiling Group*		
PostAgentProfile	Concede permiso para enviar un perfil obtenido por un agente que pertenece a un grupo de perfiles específico para agregarlo	Escritura	Profiling Group*		
PutPermission	Concede permiso para actualizar la lista de entidades principales permitidas para un grupo de acciones en la política de recursos asociada al grupo de creación de perfiles especificado	Administración de permisos	Profiling Group*		
RemoveNotificationChannel	Otorga permiso para eliminar un SNStopic arn ya configurado de la configuración de notificaciones	Escritura	Profiling Group*		
RemovePermission	Concede permiso para quitar el permiso del grupo de acciones especificado de la política de recursos asociada al grupo de perfiles especificado	Administración de permisos	Profiling Group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SubmitFeedback	Concede permiso para enviar comentarios de los usuarios sobre anomalías útiles o no útiles	Write	Profiling Group*		
TagResource	Concede permiso para agregar o sobrescribir etiquetas a un grupo de creación de perfiles	Etiquetado	Profiling Group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para quitar etiquetas de un grupo de creación de perfiles	Etiquetado	Profiling Group*		
				aws:TagKeys	
UpdateProfilingGroup	Concede permiso para actualizar un grupo de perfiles específico	Escritura	Profiling Group*		

Tipos de recursos definidos por Amazon CodeGuru Profiler

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Profiling Group	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${ProfilingGroupName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon CodeGuru Profiler

Amazon CodeGuru Profiler define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer (prefijo de servicio:`codeguru-reviewer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CodeGuru Reviewer
- Tipos de recursos definidos por Amazon CodeGuru Reviewer
- Claves de condición de Amazon CodeGuru Reviewer

Acciones definidas por Amazon CodeGuru Reviewer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate Repository	Otorga permiso para asociar un repositorio a Amazon CodeGuru Reviewer	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	codecommit:GetRepository codecommit:ListRepositories codecommit:TagResource codestar-connections:PassConnection

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					events:PutRule events:PutTargets iam:CreateServiceLinkedRole s3:CreateBucket s3:ListBucket s3:PutBucketPolicy s3:PutLifecycleConfiguration
CreateCodeReview	Concede permiso para crear una revisión de código	Write	association*		s3:GetObject
				aws:ResourceTag/${TagKey}	
CreateConnectionToken [solo permiso]	Concede permiso para realizar un protocolo de enlace oauth basado en web para proveedores de terceros	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCodeReview	Concede permiso para describir una revisión de código	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeRecommendationFeedback	Concede permiso para describir comentarios de recomendación sobre una revisión de código	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeRepositoryAssociation	Concede permiso para describir una asociación de repositorio	Lectura	association*		
				aws:ResourceTag/${TagKey}	
DisassociateRepository	Otorga permiso para desasociar un repositorio de Amazon CodeGuru Reviewer	Escritura	association*		codecommit:UntagResource events:DeleteRule events:RemoveTargets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetMetricsData [solo permiso]	Concede permiso para ver las métricas de solicitudes de extracción en la consola	Read			
ListCodeReviews	Concede permiso para mostrar un resumen de revisiones de código	List			
ListRecommendationFeedback	Concede permiso para mostrar un resumen de comentarios de recomendación sobre una revisión de código	List	association*		
				aws:ResourceTag/${TagKey}	
ListRecommendations	Concede permiso para mostrar un resumen de recomendaciones sobre una revisión de código	List	association*		
				aws:ResourceTag/${TagKey}	
ListRepositoryAssociations	Concede permiso para mostrar un resumen de asociaciones de repositorios	List			
ListTagsForResource	Concede permiso para mostrar el recurso vinculado a un ARN de repositorio asociado	List	association*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ListThirdPartyRepositories [solo permiso]	Concede permiso para mostrar los repositorios de proveedores de terceros en la consola	Read			
PutRecommendationFeedback	Concede permiso para enviar comentarios para una recomendación sobre una revisión de código	Write	association*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para vincular etiquetas de recursos a un ARN de repositorio asociado	Etiquetado	association*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagResource	Concede permiso para desasociar etiquetas de recursos de un ARN de repositorio asociado	Etiquetado	association*		
				aws:TagKeys	

Tipos de recursos definidos por Amazon CodeGuru Reviewer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
association	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}`	aws:ResourceTag/${TagKey}
codereview	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}:codereview:${CodeReviewId}`	

Claves de condición de Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon CodeGuru Security

Amazon CodeGuru Security (prefijo de servicio:`codeguru-security`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CodeGuru Security
- Tipos de recursos definidos por Amazon CodeGuru Security
- Claves de condición de Amazon CodeGuru Security

Acciones definidas por Amazon CodeGuru Security

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetFindings	Otorga permiso para recuperar por lotes los hallazgos específicos generados por la seguridad CodeGuru	Lectura	ScanName		
CreateScan	Otorga permiso para crear un escaneo CodeGuru de seguridad	Escritura	ScanName		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUploadUrl	Concede permiso para generar una URL prefirmada para cargar archivos de código	Escritura	ScanName		
DeleteScansByCategory [solo permiso]	Otorga permiso para eliminar todos los escaneos y los resultados relacionados de CodeGuru Seguridad por categoría determinada	Escritura			
GetAccountConfiguration	Concede permiso para recuperar las configuraciones de nivel de cuenta	Lectura			
GetFindings	Otorga permiso para recuperar los resultados de un escaneo generado por el	Enumeración	ScanName		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Departamento CodeGuru de Seguridad				
GetMetricsSummary	Otorga permiso para recuperar el resumen de métricas AWS a nivel de cuenta generado por Security CodeGuru	Lectura			
GetScan	Otorga permiso para recuperar los metadatos del escaneo CodeGuru de seguridad	Lectura	ScanName		
				aws:ResourceTag/${TagKey}	
ListFindings [solo permiso]	Otorga permiso para recuperar los hallazgos generados por el equipo CodeGuru de seguridad	Enumeración			
ListFindingsMetrics	Concede permiso para recuperar una lista de métricas de resultados de nivel de cuenta de un intervalo de fechas	Enumeración			
ListScans	Otorga permiso para recuperar la lista de metadatos del escaneo de CodeGuru seguridad	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para recuperar una lista de etiquetas para el ARN de nombre de un análisis	Lectura	ScanName*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para agregar etiquetas al ARN de nombre de un análisis	Etiquetado	ScanName*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas del ARN de nombre de un análisis	Etiquetado	ScanName*		
				aws:TagKeys	
UpdateAccountConfiguration	Concede permiso para actualizar las configuraciones de nivel de cuenta	Escritura			

Tipos de recursos definidos por Amazon CodeGuru Security

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ScanName	`arn:${Partition}:codeguru-security:${Region}:${Account}:scans/${ScanName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon CodeGuru Security

Amazon CodeGuru Security define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS CodePipeline

AWS CodePipeline (prefijo de servicio:`codepipeline`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodePipeline
- Tipos de recursos definidos por AWS CodePipeline
- Claves de condición de AWS CodePipeline

Acciones definidas por AWS CodePipeline

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcknowledgeJob	Otorga permiso para ver información sobre un trabajo específico y si el proceso de trabajo lo ha recibido.	Write			
AcknowledgeThirdPartyJob	Otorga permiso para confirmar que un proceso de trabajo ha recibido el trabajo especificado (solo acciones de socios)	Escritura			
CreateCustomActionType	Otorga permiso para crear una acción personalizada que puedes usar en las canalizaciones asociadas a tu Cuenta de AWS	Escritura	actiontype*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreatePipeline	Otorga permiso para crear una canalización con nombre único	Escritura	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomActionType	Otorga permiso para eliminar una acción personalizada	Write	actiontype*		
DeletePipeline	Otorga permiso para eliminar una canalización específica	Write	pipeline*		
DeleteWebhook	Otorga permiso para eliminar un webhook específico	Write	webhook*		
DeregisterWebhookWithThirdParty	Otorga permiso para eliminar el registro de un webhook con el tercero especificado en su configuración	Write	webhook*		
DisableStageTransition	Otorga permiso para evitar que las revisiones pasen a la siguiente etapa de una canalización	Write	stage*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableStageTransition	Otorga permiso para permitir que las revisiones pasen a la siguiente etapa de una canalización	Escritura	stage*		
GetActionType	Otorga permiso para obtener información sobre un tipo de acción	Lectura			
GetJobDetails	Otorga permiso para ver información sobre un trabajo (solo acciones personalizadas)	Read			
GetPipeline	Otorga permiso para recuperar información sobre una estructura de canalización	Read	pipeline*		
GetPipelineExecution	Otorga permiso para ver información sobre la ejecución de una canalización, como los detalles de los artefactos, el ID de ejecución de la canalización y el nombre, la versión y el estado de la canalización.	Read	pipeline*		
GetPipelineState	Otorga permiso para ver información sobre el estado actual de las etapas y acciones de una canalización	Read	pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetThirdPartyJobDetails	Otorga permiso para ver los detalles de un trabajo para una acción de terceros (solo acciones de socios)	Read			
ListActionExecutions	Otorga permiso para enumerar las ejecuciones de acciones que se han producido en una canalización	Read	pipeline*		
ListActionTypes	Otorga permiso para enumerar un resumen de todos los tipos de acción disponibles para las canalizaciones de su cuenta	Lectura			
ListDeployActionExecutionTargets	Otorga permiso para enumerar los detalles de despliegue de las ejecuciones de acciones de despliegue que se hayan producido en una canalización	Lectura	pipeline*		
ListPipelineExecutions	Otorga permiso para enumerar un resumen de las ejecuciones más recientes de una canalización	Enumeración	pipeline*		
ListPipelines	Otorga permiso para incluir un resumen de todas las canalizaciones asociadas a su Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRuleExecutions	Concede permiso para enumerar las ejecuciones de reglas que se han producido en una canalización	Lectura	pipeline*		
ListRuleTypes	Concede permiso para enumerar un resumen de todos los tipos de reglas disponibles para las canalizaciones de la cuenta	Lectura			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso CodePipeline	Lectura	actiontype		
			pipeline		
			webhook		
ListWebhooks	Otorga permiso para enumerar todos los webhooks asociados a tu Cuenta de AWS	Enumeración	webhook*		
OverrideStageCondition	Concede permiso para reanudar la ejecución de la canalización. Para ello, anula una condición en una etapa	Escritura	stage*		
PollForJobs	Otorga permiso para ver información sobre cualquier puesto de trabajo CodePipeline con el que poder actuar	Escritura	actiontype*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PollForThirdPartyJobs	Otorga permiso para determinar si hay trabajos de terceros en los que actúe un proceso de trabajo (solo acciones de socios)	Write			
PutActionRevision	Otorga permiso para editar acciones en una canalización	Escritura	action*		
PutApprovalResult	Otorga permiso para dar una respuesta (aprobada o rechazada) a una solicitud de aprobación manual en CodePipeline	Escritura	action*		
PutJobFailureResult	Otorga permiso para representar el error de un trabajo devuelto a la canalización por un proceso de trabajo (solo acciones personalizadas)	Write			
PutJobSuccessResult	Otorga permiso para representar el éxito de un trabajo devuelto a la canalización por un proceso de trabajo (solo acciones personalizadas)	Write			
PutThirdPartyJobFailureResult	Otorga permiso para representar el error de un trabajo de terceros devuelto a la canalización por un proceso de trabajo (solo acciones de socios)	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutThirdPartyJobSuccessResult	Otorga permiso para representar el éxito de un trabajo de terceros devuelto a la canalización por un proceso de trabajo (solo acciones de socios)	Write			
PutWebhook	Otorga permiso para crear o actualizar un webhook	Escritura	pipeline*		
			webhook*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterWebhookWithThirdParty	Otorga permiso para registrar un webhook con el tercero especificado en su configuración	Write	webhook*		
RetryStageExecution	Otorga permiso para reanudar la ejecución en la canalización reintentando las últimas acciones erróneas de una etapa	Escritura	stage*		
RollbackStage	Concede permiso para revertir la etapa a una ejecución anterior correcta	Escritura	stage*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartPipelineExecution	Otorga permiso para ejecutar la revisión más reciente a través de la canalización	Write	pipeline*		
StopPipelineExecution	Otorga permiso para detener la ejecución de una canalización en curso	Escritura	pipeline*		
TagResource	Otorga permiso para etiquetar un CodePipeline recurso	Etiquetado	actiontype		
			pipeline		
			webhook		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una etiqueta de un CodePipeline recurso	Etiquetado	actiontype		
			pipeline		
			webhook		
				aws:TagKeys	
UpdateActionType	Otorga permiso para actualizar un tipo de acción	Escritura	actiontype*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePipeline	Otorga permiso para actualizar una canalización con cambios en la estructura de la canalización	Escritura	pipeline*		

Tipos de recursos definidos por AWS CodePipeline

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
action	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}`	aws:ResourceTag/${TagKey}
actiontype	`arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}`	aws:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}`	aws:ResourceTag/${TagKey}
stage	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
webhook	`arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS CodePipeline

AWS CodePipeline define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS CodeStar

AWS CodeStar (prefijo de servicio:`codestar`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS CodeStar
- Tipos de recursos definidos por AWS CodeStar
- Claves de condición de AWS CodeStar

Acciones definidas por AWS CodeStar

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateTeamMember	Otorga permiso para añadir un usuario al equipo de un proyecto AWS CodeStar	Administración de permisos	project*		
CreateProject	Concede permiso para crear un proyecto con estructura mínima, políticas de cliente y ningún recurso	Administración de permisos		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Concede permiso para crear un perfil para un usuario que incluye las preferencias, el nombre de visualización y el correo electrónico	Escritura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteExtendedAccess [solo permiso]	Otorga permiso para la eliminación prolongada APIs	Escritura	project*		
DeleteProject	Concede permiso para eliminar un proyecto, incluidos sus recursos No elimina los usuarios asociados con el proyecto, pero elimina los roles de IAM que permitían el acceso al proyecto	Administración de permisos	project*		
DeleteUserProfile	Otorga permiso para eliminar un perfil de usuario en AWS CodeStar, incluidos todos los datos de preferencias personales asociados a ese perfil, como el nombre para mostrar y la dirección de correo electrónico. No elimina el historial de ese usuario; por ejemplo, el historial de confirmaciones que hizo dicho usuario	Escritura	user*		
DescribeProject	Concede permiso para describir un proyecto y sus recursos	Lectura	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeUserProfile	Otorga permiso para describir a un usuario AWS CodeStar y sus atributos en todos los proyectos	Lectura			
DisassociateTeamMember	Concede permiso para eliminar un usuario de un proyecto. Cuando se elimina a un usuario de un proyecto también se eliminan las políticas de IAM de ese usuario que le daban acceso al proyecto y sus recursos	Administración de permisos	project*		
GetExtendedAccess [solo permiso]	Otorga permiso de lectura prolongada APIs	Lectura	project*		
ListProjects	Otorga permiso para enumerar todos los proyectos CodeStar asociados a su Cuenta de AWS	Enumeración			
ListResources	Otorga permiso para enumerar todos los recursos asociados a un proyecto en CodeStar	Enumeración	project*		
ListTagsForProject	Otorga permiso para incluir las etiquetas asociadas a un proyecto en CodeStar	Enumeración	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTeamMembers	Concede permiso para enumerar todos los miembros de un equipo asociados a un proyecto	Enumeración	project*		
ListUserProfiles	Otorga permiso para incluir perfiles de usuario en AWS CodeStar	Enumeración			
PutExtendedAccess [solo permiso]	Otorga permiso de escritura prolongada APIs	Escritura	project*		
TagProject	Otorga permiso para añadir etiquetas a un proyecto en CodeStar	Etiquetado	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagProject	Otorga permiso para eliminar etiquetas de un proyecto en CodeStar	Etiquetado	project*		
				aws:TagKeys	
UpdateProject	Otorga permiso para actualizar un proyecto en CodeStar	Escritura	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTeamMember	Otorga permiso para actualizar los atributos de los miembros del equipo dentro de un CodeStar proyecto	Administración de permisos	project*		
UpdateUserProfile	Concede permiso para actualizar un perfil para un usuario que incluye las preferencias, el nombre de visualización y el correo electrónico	Escritura	user*		
VerifyServiceRole	Otorga permiso para verificar si el rol de AWS CodeStar servicio existe en la cuenta del cliente	Enumeración			

Tipos de recursos definidos por AWS CodeStar

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
project	`arn:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
user	arn:${Partition}:iam::${Account}:user/${AwsUserName}	iam:ResourceTag/${TagKey}

Claves de condición de AWS CodeStar

AWS CodeStar define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por solicitudes en función del conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por acciones en función del valor de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra el acceso por solicitudes en función de la presencia de las etiquetas obligatorias en la solicitud	ArrayOfString
iam:ResourceTag/${TagKey}	Filtra el acceso por acciones en función del valor de la etiqueta asociada con el recurso	Cadena

Claves de condición, recursos y acciones de AWS CodeStar Connections

AWS CodeStar Connections (prefijo de servicio:`codestar-connections`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Connections AWS CodeStar
- Tipos de recursos definidos por AWS CodeStar Connections
- Claves de condición para AWS CodeStar las conexiones

Acciones definidas por Connections AWS CodeStar

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnection	Concede permiso para crear un recurso Connection	Write		aws:RequestTag/${TagKey} aws:TagKeys codestar-connectio	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ns:ProviderType	
CreateHost	Concede permiso para crear un recurso de host	Escritura		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType codestar-connections:VpcId	
CreateRepositoryLink	Otorga permiso para crear un enlace de repositorio	Escritura	Connection*		codestar-connections:PassConnection codestar-connections:UseConnection

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Otorga permiso para crear una configuración de plantilla sincronizada	Escritura	RepositoryLink*		codestar-connections:PassRepository iam:PassRole
				codestar-connections:Branch	
DeleteConnection	Concede permiso para eliminar un recurso Connection	Write	Connection*		
DeleteHost	Concede permiso para eliminar un recurso de host	Escritura	Host*		
DeleteRepositoryLink	Otorga permiso para eliminar un enlace de repositorio	Escritura	RepositoryLink*		
DeleteSyncConfiguration	Otorga permiso para eliminar una configuración de sincronización	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnection	Concede permiso para obtener detalles sobre un recurso Connection	Lectura	Connection*		
GetConnectionToken [solo permiso]	Concede permiso para obtener un token de conexión para llamar a las acciones del proveedor	Lectura	Connection*		
GetHost	Concede permiso para obtener información detallada acerca de un recurso de host	Read	Host*		
GetIndividualAccessToken [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Read		codestar-connections:ProviderType	codestar-connections:StartOAuthHandshake
GetInstallationUrl [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Lectura		codestar-connections:ProviderType	
GetRepositoryLink	Otorga permiso para describir un enlace de repositorio	Lectura	RepositoryLink*		
GetRepositorySyncStatus	Otorga permiso para obtener el estado de sincronización más reciente de un repositorio	Lectura	RepositoryLink*		
				codestar-connections:Branch	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourceSyncStatus	Concede permiso para obtener el estado de sincronización más reciente de un recurso (pila cfn u otros recursos)	Lectura			
GetSyncBlockerSummary	Concede permiso para describir los bloqueadores de sincronización de servicio en un recurso (pila cfn u otros recursos)	Lectura			
GetSyncConfiguration	Concede permiso para describir una configuración de sincronización	Lectura			
ListConnections	Concede permiso para enumerar los recursos Connection	List	Connection*		
				codestar-connections:ProviderTypeFilter	
ListHosts	Concede permiso para mostrar los recursos de host	List		codestar-connections:ProviderTypeFilter	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListInstallationTargets [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Enumeración			codestar-connections:GetIndividualAccessToken codestar-connections:StartOAuthHandshake
ListRepositoryLinks	Otorga permiso para enumerar enlaces de repositorios	Enumeración			
ListRepositorySyncDefinitions	Otorga permiso para enumerar definiciones de sincronización de repositorios	Enumeración			
ListSyncConfigurations	Concede permiso para mostrar una lista de las configuraciones de sincronización para un enlace de repositorio	Enumeración			
ListTagsForResource	Concede permiso al conjunto de pares de clave-valor que se utiliza para administrar el recurso	Enumeración	Connection		
			Host		
			RepositoryLink		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PassConnection [solo permiso]	Otorga permiso para pasar un recurso de conexión a un AWS servicio que acepta un ARN de conexión como entrada, como codepipeline: CreatePipeline	Lectura	Connection*		
				codestar-connections:PassedToService	
PassRepository [solo permiso]	Otorga permiso para pasar un recurso de enlace de repositorio a un AWS servicio que acepta un RepositoryLinkId como entrada, como codestar-connections: CreateSyncConfiguration	Lectura	RepositoryLink*		
				codestar-connections:PassedToService	
RegisterAppCode [solo permiso]	Otorga permiso para asociar un servidor de terceros, como una instancia de GitHub Enterprise Server, a un host	Lectura		codestar-connections:HostArn	
StartAppRegistrationHandshake [solo permiso]	Otorga permiso para asociar un servidor de terceros, como una instancia de GitHub Enterprise Server, a un host	Lectura		codestar-connections:HostArn	
StartOAuthHandshake [solo permiso]	Concede permiso para asociar a un tercero, como una instalación de Bitbucket App, a un recurso Connection	Lectura		codestar-connections:ProviderType	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para agregar o modificar las etiquetas del recurso especificado.	Etiquetado	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un AWS recurso	Etiquetado	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnectionInstallation	Otorga permiso para actualizar un recurso de Connection con una instalación de la aplicación CodeStar Connections	Escritura	Connection*		codestar-connections:GetIndividualAccessToken codestar-connections:GetInstallationUrl codestar-connections:ListInstallationTargets codestar-connections:StartOAuthHandshake
				codestar-connections:InstallationId	
UpdateHost	Concede permiso para actualizar un recurso de host.	Escritura	Host*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				codestar-connections:VpcId	
UpdateRepositoryLink	Otorga permiso para actualizar un enlace de repositorio	Escritura	RepositoryLink*		
UpdateSyncBlocker	Otorga permiso para actualizar un bloqueador de sincronización para un recurso (pila cfn u otros recursos)	Escritura			
UpdateSyncConfiguration	Otorga permiso para actualizar una configuración de sincronización	Escritura		codestar-connections:Branch	
UseConnection [solo permiso]	Concede permiso para usar un recurso Connection para llamar a acciones del proveedor	Lectura	Connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				codestar-connections:BranchName codestar-connections:FullRepositoryId codestar-connections:OwnerId codestar-connections:ProviderAction codestar-connections:ProviderPermissionsRequired codestar-connections:RepositoryName	

Tipos de recursos definidos por AWS CodeStar Connections

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Connection	`arn:${Partition}:codestar-connections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codestar-connections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codestar-connections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS CodeStar las conexiones

AWS CodeStar Connections define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
codestar-connections:Branch	Filtra el acceso por el nombre de ramificación que se incluye en la solicitud	Cadena
codestar-connections:BranchName	Filtra el acceso por el nombre de ramificación que se incluye en la solicitud. Se aplica solo a UseConnection las solicitudes de acceso a una rama de repositorio específica	Cadena
codestar-connections:FullRepositoryId	Filtra el acceso del repositorio que se incluye en la solicitud. Se aplica solo a UseConnection las solicitudes de acceso a un repositorio específico	Cadena
codestar-connections:HostArn	Filtra el acceso por el recurso de host asociado a la conexión utilizada en la solicitud	ARN
codestar-connections:InstallationId	Filtra el acceso por el ID de terceros (como el ID de instalación de la aplicación Bitbucket para CodeStar las conexiones) que se utiliza para actualizar una conexión. Le permite restringir las instalaciones de aplicaciones de terceros que se pueden utilizar para realizar una Connection	Cadena

Claves de condición	Descripción	Tipo
codestar-connections:OwnerId	Filtra el acceso por propietario del repositorio de terceros. Se aplica solo a UseConnection las solicitudes de acceso a los repositorios propiedad de un usuario específico	Cadena
codestar-connections:PassedToService	Filtra el acceso por el servicio al que el principal puede transferir una conexión o RepositoryLink	Cadena
codestar-connections:ProviderAction	Filtra el acceso por la acción del proveedor en una UseConnection solicitud como ListRepositories. Consulte la documentación para ver todos los valores válidos	Cadena
codestar-connections:ProviderPermissionsRequired	Filtra el acceso mediante los permisos de escritura de una acción del proveedor en una UseConnection solicitud . Los tipos válidos son read_only y read_write	Cadena
codestar-connections:ProviderType	Filtra el acceso por el tipo de proveedor externo incluido en la solicitud	Cadena
codestar-connections:ProviderTypeFilter	Filtra el acceso por el tipo de proveedor externo utilizado para filtrar resultados	Cadena
codestar-connections:RepositoryName	Filtra el acceso por el nombre del repositorio que se incluye en la solicitud. Solo se aplica a UseConnection las solicitudes de acceso a los repositorios propiedad de un usuario específico	Cadena

Claves de condición	Descripción	Tipo
codestar-connections:VpcId	Filtra el acceso según lo VpcId aprobado en la solicitud	Cadena

Claves de condición, recursos y acciones de las AWS CodeStar notificaciones

AWS CodeStar Las notificaciones (prefijo de servicio:`codestar-notifications`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las notificaciones AWS CodeStar
- Tipos de recursos definidos por AWS CodeStar las notificaciones
- Claves de condición para AWS CodeStar las notificaciones

Acciones definidas por las notificaciones AWS CodeStar

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNotificationRule	Otorga permisos para crear una regla de notificación para un recurso	Write	notificationrule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteNotificationRule	Otorga permisos para eliminar una regla de notificación de un recurso	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				codestar-notifications:NotificationsForResource	
DeleteTarget	Otorga permisos para eliminar un destino para una regla de notificación	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DescribeNotificationRule	Otorga permisos para obtener información sobre una regla de notificación	Read	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEventTypes	Otorga permisos para enumerar los tipos de eventos de notificaciones	Enumeración			
ListNotificationRules	Otorga permiso para enumerar las reglas de notificación en un Cuenta de AWS	Enumeración			
ListTagsForResource	Otorga permisos para enumerar las etiquetas asociadas a un recurso de regla de notificación ARN	Enumeración	notificationrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTargets	Otorga permiso para enumerar los objetivos de las reglas de notificación de un Cuenta de AWS	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
Subscribe	Otorga permisos para crear una asociación entre una regla de notificación y un tema de Amazon SNS	Write	notificationrule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
TagResource	Otorga permisos para adjuntar etiquetas de recurso a un recurso de regla de notificación ARN	Etiquetado	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Unsubscribe	Otorga permisos para eliminar una asociación entre una regla de notificación y un tema de Amazon SNS	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
UntagResource	Otorga permisos para desasociar etiquetas de recurso de un recurso de regla de notificación ARN	Etiquetado	notificationrule*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateNotificationRule	Otorga permisos para cambiar una regla de notificación de un recurso	Escritura	notificationrule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Tipos de recursos definidos por AWS CodeStar las notificaciones

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
notificationrule	`arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS CodeStar las notificaciones

AWS CodeStar Las notificaciones definen las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString
codestar-notifications:NotificationsForResource	Filtra el acceso basado en el ARN del recurso para el que se configuran las notificaciones	ARN

Acciones, recursos y claves de condición de Amazon CodeWhisperer

Amazon CodeWhisperer (prefijo de servicio:`codewhisperer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon CodeWhisperer
- Tipos de recursos definidos por Amazon CodeWhisperer
- Claves de estado de Amazon CodeWhisperer

Acciones definidas por Amazon CodeWhisperer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Otorga permiso para configurar la entrega de registros vendida como recurso de personalización CodeWhisperer	Administración de permisos	customization*		
				aws:ResourceTag/${TagKey}	
AssociateCustomizationPermi	Otorga permiso para invocar on AssociateCustomiza	Escritura	customization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ssion [solo permiso]	tionPermission CodeWhisperer			aws:ResourceTag/${TagKey}	
CreateCustomization [solo permiso]	Otorga permiso para CreateCustomization invocar a CodeWhisperer	Escritura	customization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile [solo permiso]	Otorga permiso para CreateProfile invocar a CodeWhisperer	Escritura	profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCustomization [solo permiso]	Otorga permiso para DeleteCustomization invocar a CodeWhisperer	Escritura	customization*		
				aws:ResourceTag/${TagKey}	
DeleteProfile [solo permiso]	Otorga permiso para DeleteProfile invocar a CodeWhisperer	Escritura	profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DisassociateCustomizationPermission [solo permiso]	Otorga permiso para DisassociateCustomizationPermission invocar a CodeWhisperer	Escritura	customization*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations [solo permiso]	Otorga permiso para GenerateRecommendations invocar a CodeWhisperer	Lectura			
GetCustomization [solo permiso]	Otorga permiso para GetCustomization invocar a CodeWhisperer	Lectura	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationPermissions [solo permiso]	Otorga permiso para ListCustomizationPermissions invocar a CodeWhisperer	Enumeración	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationVersions [solo permiso]	Otorga permiso para ListCustomizationVersions invocar a CodeWhisperer	Enumeración	customization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ListCustomizations [solo permiso]	Otorga permiso para ListCustomizations invocar a CodeWhisperer	Enumeración	customization*		
ListProfiles [solo permiso]	Otorga permiso para ListProfiles invocar a CodeWhisperer	Enumeración			
ListTagsForResource [solo permiso]	Otorga permiso para ListTagsForResource invocar a CodeWhisperer	Enumeración	customization		
			profile		
				aws:ResourceTag/${TagKey}	
TagResource [solo permiso]	Otorga permiso para TagResource invocar a CodeWhisperer	Etiquetado	customization		
			profile		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [solo permiso]	Otorga permiso para UntagResource invocar a CodeWhisperer	Etiquetado	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCustomization [solo permiso]	Otorga permiso para UpdateCustomization invocar a CodeWhisperer	Escritura	customization*		
				aws:ResourceTag/${TagKey}	
UpdateProfile [solo permiso]	Otorga permiso para UpdateProfile invocar a CodeWhisperer	Escritura	profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon CodeWhisperer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	aws:ResourceTag/${TagKey}
customization	`arn:${Partition}:codewhisperer:${Region}:${Account}:customization/${Identifier}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon CodeWhisperer

Amazon CodeWhisperer define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al CodeWhisperer recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Cognito Identity

Amazon Cognito Identity (prefijo de servicio: `cognito-identity`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por identidad de Amazon Cognito
- Tipos de recurso definidos por Amazon Cognito Identity
- Claves de condición de identidad de Amazon Cognito

Acciones definidas por identidad de Amazon Cognito

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIdentityPool	Otorga permiso para crear un grupo de identidades.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	Otorga permiso para eliminar identidades de un grupo de identidades. Puede especificar una lista de 1-60 identidades que desee eliminar.	Write			
DeleteIdentityPool	Otorga permiso para eliminar un grupo de usuarios. Una vez que un grupo se elimina, los usuarios no pueden autenticarse con el grupo.	Write	identitypool*		
DescribeIdentity	Otorga permiso para devolver los metadatos relacionados con la identidad determinada, incluido cuando se creó la identidad y los inicios de sesión vinculados y asociados.	Read			
DescribeIdentityPool	Otorga permiso para obtener información detallada acerca de un determinado grupo	Read	identitypool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de identidades, incluido el nombre de grupo, la descripción de ID, la fecha de creación y el número actual de usuarios.				
GetCredentialsForIdentity	Otorga permiso para devolver credenciales para el ID de identidad proporcionado.	Read			
GetId	Otorga permiso para generar (o recuperar) un ID de Cognito. Suministrar varios inicios de sesión creará una cuenta vinculada implícita.	Escritura			
GetIdentityPoolAnalytics	Otorga permiso para obtener datos analíticos sobre el recuento total de identidades actual de todos los proveedores de identidades del grupo de identidades () IdPs	Lectura	identitypool*		
GetIdentityPoolDailyAnalytics	Otorga permiso para obtener datos analíticos sobre el número de identidades nuevas y el total de identidades de todos los proveedores de identidades del grupo de identidades (IdPs)	Lectura	identitypool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIdentityPoolRoles	Otorga permiso para obtener los roles de un grupo de identidades.	Lectura	identitypool*		
GetIdentityProviderDailyAnalytics	Otorga permiso para obtener datos analíticos sobre el número de identidades nuevas y el total de identidades de un proveedor de identidades (IdPs)	Lectura	identitypool*		
GetOpenIdToken	Otorga permiso para obtener un token OpenID con un ID de Cognito conocido	Lectura			
GetOpenIdTokenForDeveloperIdentity	Otorga permiso para registrar (o recuperar) un token de Cognito IdentityId y un token de OpenID Connect para un usuario autenticado mediante su proceso de autenticación de backend	Lectura	identitypool*		
GetPrincipalTagAttributeMap	Otorga permiso para obtener las etiquetas principales para un grupo de identidades y un proveedor.	Read	identitypool*		
ListIdentities	Otorga permiso para enumerar las identidades de un grupo de identidades.	List	identitypool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIdentityPools	Otorga permiso para enumerar todos los grupos de identidades de Cognito registrados en la cuenta.	List			
ListTagsForResource	Otorga permiso para enumerar las etiquetas asignadas a un grupo de identidades de Amazon Cognito.	Lectura	identitypool		
LookupDeveloperIdentity	Otorga permiso para recuperar la IdentityId identidad asociada a una DeveloperUserIdentifier o la lista de entidades Developer UserIdentifiers asociadas a una identidad existente IdentityId	Lectura	identitypool*		
MergeDeveloperIdentities	Otorga permiso para combinar dos usuarios que tienen identidades diferentes IdentityIds, que existen en el mismo grupo de identidades e identificados por el mismo proveedor desarrollador	Escritura	identitypool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetIdentityPoolRoles	Otorga permiso para establecer los roles de un grupo de identidades. Estas funciones se utilizan al realizar llamadas a la GetCredentialsForIdentity acción	Escritura			
SetPrincipalTagAttributeMap	Otorga permiso para establecer las etiquetas principales para un grupo de identidades y un proveedor . Estas etiquetas se utilizan al realizar llamadas a la GetOpenIdToken acción	Escritura			
TagResource	Otorga permiso para asignar un conjunto de etiquetas a un grupo de identidades de Amazon Cognito.	Etiquetado	identitypool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnlinkDeveloperIdentity	Otorga permiso para desvincular DeveloperUserIdentifier a de una identidad existente	Escritura	identitypool*		
UnlinkIdentity	Otorga permiso para desvincular una identidad federada de una cuenta existente.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar las etiquetas especificadas a partir de un grupo de identidades de Amazon Cognito.	Etiquetado	identitypool		
				aws:TagKeys	
UpdateIdentityPool	Otorga permiso para actualizar un grupo de identidades.	Write	identitypool*		

Tipos de recurso definidos por Amazon Cognito Identity

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
identitypool	`arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}`	aws:ResourceTag/${TagKey}

Claves de condición de identidad de Amazon Cognito

Amazon Cognito Identity define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por una clave que está presente en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para Amazon Cognito Sync

Amazon Cognito Sync (prefijo de servicio: `cognito-sync`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Cognito Sync
- Tipos de recurso definidos por Amazon Cognito Sync
- Claves de condición de Amazon Cognito Sync

Acciones definidas por Amazon Cognito Sync

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BulkPublish	Concede permiso para iniciar una publicación en masa de todos los conjuntos de datos existentes para un grupo de identidades en el flujo configurado	Escritura	identitypool*		
DeleteDataset	Concede permiso para eliminar un conjunto de datos específico	Escritura	dataset*		
DescribeDataset	Concede permiso para obtener metadatos acerca de un conjunto de datos mediante el nombre de conjunto de datos e identidad	Lectura	dataset*		
DescribeIdentityPoolUsage	Concede permiso para obtener detalles de uso (por ejemplo, almacenamiento de datos) acerca de un grupo de identidades determinado	Lectura	identitypool*		
DescribeIdentityUsage	Concede permiso para obtener información de uso para una identidad, incluido el nombre de conjuntos de datos y uso de datos	Lectura	identity*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBulkPublishDetails	Otorga permiso para obtener el estado de la última BulkPublish operación de un grupo de identidades	Lectura	identitypool*		
GetCognitoEvents	Concede permiso para obtener los eventos y las funciones Lambda correspondientes asociadas a un grupo de identidades	Lectura	identitypool*		
GetIdentityPoolConfiguration	Concede permiso para obtener la configuración de un grupo de identidades	Lectura	identitypool*		
ListDatasets	Concede permiso para enumerar conjuntos de datos para una identidad	Enumeración	dataset*		
ListIdentityPoolUsage	Concede permiso para obtener una lista de grupos de identidades registrados con Cognito.	Lectura	identitypool*		
ListRecords	Concede permiso para obtener registros paginados, opcionalmente cambiados después de un recuento de sincronización determinado para una identidad y conjunto de datos	Lectura	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
QueryRecords [solo permiso]	Concede permiso para consultar registros	Lectura			
RegisterDevice	Concede permiso para registrar un dispositivo para recibir notificaciones de sincronización mediante inserción	Escritura	identity*		
SetCognitoEvents	Otorga permiso para configurar la función AWS Lambda para un tipo de evento determinado de un grupo de identidades	Escritura	identitypool*		
SetDatasetConfiguration [solo permiso]	Concede permiso para configurar conjuntos de datos	Escritura	dataset*		
SetIdentityPoolConfiguration	Concede permiso para establecer la configuración necesaria para la sincronización mediante inserción	Escritura	identitypool*		
SubscribeToDataset	Concede permiso para suscribirse para recibir notificaciones cuando otro dispositivo modifica un conjunto de datos	Escritura	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UnsubscribeFromDataset	Concede permiso para suscribirse de las notificaciones de recepción cuando otro dispositivo modifica un conjunto de datos	Escritura	dataset*		
UpdateRecords	Concede permiso para publicar actualizaciones en los registros, y agrega y elimina registros para un conjunto de datos y usuario	Escritura	dataset*		

Tipos de recurso definidos por Amazon Cognito Sync

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	

Tipos de recurso	ARN	Claves de condición
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	
identitypool	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}`	

Claves de condición de Amazon Cognito Sync

Cognito Sync no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para los grupos de usuarios de Amazon Cognito

Grupos de usuarios de Amazon Cognito (prefijo de servicio: `cognito-idp`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por los grupos de usuarios de Amazon Cognito
- Tipos de recurso definidos por los grupos de usuarios de Amazon Cognito
- Claves de condición de los grupos de usuarios de Amazon Cognito

Acciones definidas por los grupos de usuarios de Amazon Cognito

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddCustomAttributes	Concede permiso para agregar atributos de usuario al esquema del grupo de usuarios	Escritura	userpool*		
AdminAddUserToGroup	Concede permiso para agregar cualquier usuario a cualquier grupo	Escritura	userpool*		
AdminConfirmSignUp	Concede permiso para confirmar el registro de cualquier usuario sin un código de confirmación	Escritura	userpool*		
AdminCreateUser	Concede permiso para crear nuevos usuarios y enviar mensajes de bienvenida por correo electrónico o SMS	Escritura	userpool*		
AdminDeleteUser	Concede permiso para eliminar cualquier usuario	Escritura	userpool*		
AdminDeleteUserAttributes	Concede permiso para eliminar atributos de cualquier usuario	Escritura	userpool*		
AdminDisableProviderForUser	Concede permiso para desvincular cualquier grupo de usuarios del grupo de usuarios	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de un proveedor de identidades (IdP) externo				
AdminDisableUser	Concede permiso para desactivar cualquier usuario	Escritura	userpool*		
AdminEnableUser	Concede permiso para activar cualquier usuario	Escritura	userpool*		
AdminForgetDevice	Concede permiso para anular el registro de los dispositivos de cualquier usuario	Escritura	userpool*		
AdminGetDevice	Concede permiso para obtener información sobre los dispositivos de cualquier usuario	Lectura	userpool*		
AdminGetUser	Concede permiso para buscar cualquier usuario por nombre de usuario	Lectura	userpool*		
AdminInitiateAuth	Concede permiso para autenticar cualquier usuario	Escritura	userpool*		
AdminLinkProviderForUser	Concede permiso para vincular cualquier grupo de usuarios con un usuario de un IdP externo	Escritura	userpool*		
AdminListDevices	Concede permiso para enumerar dispositivos recordados por cualquier usuario	Enumeración	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AdminListGroupsForUser	Concede permiso para enumerar los grupos a los que pertenece cualquier usuario	Enumeración	userpool*		
AdminListUserAuthEvents	Concede permiso para enumerar eventos de inicio de sesión para cualquier usuario	Lectura	userpool*		
AdminRemoveUserFromGroup	Concede permiso para eliminar un usuario de cualquier grupo	Escritura	userpool*		
AdminResetUserPassword	Concede permiso para restablecer la contraseña de cualquier usuario	Escritura	userpool*		
AdminRespondToAuthChallenge	Concede permiso para responder a un desafío de autenticación durante la autenticación de cualquier usuario	Escritura	userpool*		
AdminSetUserMFAPreference	Concede permiso para establecer el método de MFA preferido de cualquier usuario	Escritura	userpool*		
AdminSetUserPassword	Concede permiso para establecer la contraseña de cualquier usuario	Escritura	userpool*		
AdminSetUserSettings	Concede permiso para establecer la configuración de usuario para cualquier usuario	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AdminUpdateAuthEventFeedback	Concede permiso para actualizar los comentarios de seguridad avanzados para cualquier evento de autenticación de usuario	Escritura	userpool*		
AdminUpdateDeviceStatus	Concede permiso para actualizar el estado de cualquier dispositivo recordado por cualquier usuario	Escritura	userpool*		
AdminUpdateUserAttributes	Concede permiso para actualizar los atributos estándar o personalizados de cualquier usuario	Escritura	userpool*		
AdminUserGlobalSignOut	Concede permiso para cerrar la sesión de cualquier usuario en todas las sesiones	Escritura	userpool*		
AssociateSoftwareToken	Otorga permiso para devolver un código único de clave secreta compartida generado para el usuario	Escritura			
AssociateWebACL [solo permiso]	Otorga permiso para asociar el grupo de usuarios a una ACL web de AWS WAF	Escritura	userpool* webacl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ChangePassword	Otorga permiso para cambiar la contraseña de un usuario específico en un grupo de usuarios	Escritura			
ConfirmDevice	Otorga permiso para confirmar el seguimiento del dispositivo. Esta llamada a la API es la llamada que comienza el seguimiento de dispositivos	Escritura			
ConfirmForgotPassword	Otorga permiso para permitir a un usuario ingresar un código de confirmación a fin de restablecer una contraseña olvidada	Escritura			
ConfirmSignUp	Otorga permiso para confirma el registro de un usuario y gestiona el alias existente de un usuario anterior	Escritura			
CreateGroup	Concede permiso para crear nuevos grupos de usuarios	Escritura	userpool*		
CreateIdentityProvider	Concede permiso para agregar proveedores de identidad a grupos de usuarios	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateManagedLoginBranding	Otorga permiso para crear una configuración de marca para el inicio de sesión gestionado y asociarla a un cliente de aplicaciones	Escritura	userpool*		
CreateResourceServer	Otorga permiso para crear y configurar ámbitos para servidores de recursos OAuth 2.0	Escritura	userpool*		
CreateUserImportJob	Concede permiso para crear trabajos de importación CSV de usuario	Escritura	userpool*		
CreateUserPool	Concede permiso para crear y establecer políticas de contraseñas para grupos de usuarios	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateUserPoolClient	Concede permiso para crear clientes de aplicaciones para grupos de usuarios	Escritura	userpool*		
CreateUserPoolDomain	Concede permiso para agregar dominios de grupos de usuarios	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteGroup	Concede permiso para eliminar cualquier grupo de usuarios vacío	Escritura	userpool*		
DeleteIdentityProvider	Concede permiso para eliminar cualquier proveedor de identidades de grupos de usuarios	Escritura	userpool*		
DeleteManagedLoginBranding	Otorga permiso para eliminar el estilo de marca de inicio de sesión administrado de cualquier cliente de aplicación	Escritura	userpool*		
DeleteResourceServer	Otorga permiso para eliminar cualquier servidor de recursos OAuth 2.0 de los grupos de usuarios	Escritura	userpool*		
DeleteUser	Otorga permiso para permitir que un usuario se elimine a sí mismo	Escritura			
DeleteUserAttributes	Otorga permiso para eliminar los atributos de un usuario	Escritura			
DeleteUserPool	Concede permiso para eliminar grupos de usuario	Escritura	userpool*		
DeleteUserPoolClient	Concede permiso para eliminar cualquier cliente de aplicación de grupos de usuarios	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUserPoolDomain	Concede permiso para eliminar cualquier dominio de grupos de usuarios	Escritura	userpool*		
DescribeIdentityProvider	Concede permiso para describir cualquier proveedor de identidades de grupos de usuarios	Lectura	userpool*		
DescribeManagedLoginBranding	Otorga permiso para obtener información detallada sobre el estilo de marca del inicio de sesión gestionado	Lectura	userpool*		
DescribeManagedLoginBrandingByClient	Otorga permiso para obtener información detallada sobre el estilo de marca del inicio de sesión administrado asociado a una app/cliente	Lectura	userpool*		
DescribeResourceServer	Otorga permiso para describir cualquier servidor de recursos OAuth 2.0	Lectura	userpool*		
DescribeRiskConfiguration	Concede permiso para describir la configuración de riesgos de los grupos de usuarios y los clientes de aplicaciones	Lectura	userpool*		
DescribeUserImportJob	Concede permiso para describir cualquier trabajo de importación de usuarios	Lectura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeUserPool	Concede permiso para describir grupos de usuarios	Lectura	userpool*		
DescribeUserPoolClient	Concede permiso para describir cualquier cliente de aplicación de grupos de usuarios	Lectura	userpool*		
DescribeUserPoolDomain	Concede permiso para describir cualquier dominio de grupos de usuarios	Lectura			
DisassociateWebACL [solo permiso]	Otorga permiso para desasociar el grupo de usuarios con una ACL web de AWS WAF	Escritura	userpool*		
ForgetDevice	Otorga permiso para olvidar el dispositivo especificado	Escritura			
ForgotPassword	Otorga permiso para enviar un mensaje al usuario final con un código de confirmación que es necesario a fin de cambiar la contraseña del usuario	Escritura			
GetCSVHeader	Concede permiso para generar encabezados para un archivo .csv de importación de usuarios	Lectura	userpool*		
GetDevice	Otorga permiso para obtener el dispositivo	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGroup	Concede permiso para describir un grupo de usuarios	Lectura	userpool*		
GetIdentityProviderByIdentifier	Concede permiso para correlacionar un identificador de IdP de grupo de usuarios con el nombre del IdP	Lectura	userpool*		
GetLogDeliveryConfiguration	Otorga permiso para obtener la configuración detallada del registro de actividades de un grupo de usuarios	Lectura	userpool*		
GetSigningCertificate	Concede permiso para buscar certificados de firma para grupos de usuarios	Lectura	userpool*		
GetTokensFromRefreshToken	Otorga permiso para actualizar los tokens de usuario con los tokens de actualización	Escritura			
GetUICustomization	Concede permiso para obtener información de personalización de la IU para la IU alojada de cualquier cliente	Lectura	userpool*		
GetUser	Otorga permiso para obtener los atributos de usuario y los metadatos de un usuario	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetUserAttributeVerificationCode	Otorga permiso para obtener el código de verificación del atributo de usuario del nombre de atributo especificado	Lectura			
GetUserPoolMfaConfig	Concede permiso para buscar la configuración MFA de grupos de usuarios	Lectura	userpool*		
GetWebACLForResource [solo permiso]	Otorga permiso para obtener la ACL web de AWS WAF asociada a un grupo de usuarios de Amazon Cognito	Lectura	userpool*		
GlobalSignOut	Otorga permiso para cerrar la sesión de los usuarios en todos los dispositivos	Escritura			
InitiateAuth	Otorga permiso para iniciar el flujo de autenticación	Escritura			
ListDevices	Otorga permiso para enumerar los dispositivos	Enumeración			
ListGroups	Concede permiso para enumerar todos los grupos en grupos de usuarios	Enumeración	userpool*		
ListIdentityProviders	Concede permiso para enumerar todos los proveedores de identidad en grupos de usuarios	Enumeración	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourceServers	Concede permiso para enumerar todos los servidores de recursos en grupos de usuarios	Enumeración	userpool*		
ListResourcesForWebACL [solo permiso]	Otorga permiso para enumerar los grupos de usuarios asociados a una ACL web de AWS WAF	Enumeración	webacl*		
ListTagsForResource	Concede permiso para enumerar las etiquetas asignadas a un grupo de usuarios de Amazon Cognito	Enumeración	userpool		
ListUserImportJobs	Concede permiso para enumerar todos los trabajos de importación de usuarios	Enumeración	userpool*		
ListUserPoolClients	Concede permiso para enumerar todos los clientes de aplicaciones en grupos de usuarios	Enumeración	userpool*		
ListUserPools	Concede permiso para enumerar todos los grupos de usuarios	Enumeración			
ListUsers	Concede permiso para enumerar todos los usuarios de grupos de usuarios	Enumeración	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListUsersInGroup	Concede permiso para enumerar a los usuarios de cualquier grupo	Enumeración	userpool*		
ResendConfirmationCode	Otorga permiso para reenviar la confirmación (del registro) a un usuario específico en el grupo de usuarios	Escritura			
RespondToAuthChallenge	Otorga permiso para responder al desafío de autenticación	Escritura			
RevokeToken	Otorga permiso para invalidar todos los tokens de acceso generados por el token de actualización especificado	Escritura			
SetLogDeliveryConfiguration	Otorga permiso para configurar o modificar la configuración detallada del registro de actividades de un grupo de usuarios	Escritura	userpool*		
SetRiskConfiguration	Concede permiso para establecer la configuración de riesgos para grupos de usuarios y clientes de aplicaciones	Escritura	userpool*		
SetUICustomization	Concede permiso para personalizar la IU alojada para cualquier cliente de aplicación	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetUserMFAPreference	Otorga permiso para establecer la preferencia de MFA del usuario del grupo de usuarios	Escritura			
SetUserPoolMfaConfig	Concede permiso para actualizar la configuración MFA de un grupo de usuarios	Escritura	userpool*		
SetUserSettings	Otorga permiso para establecer la configuración del usuario como autenticación multifactor (MFA)	Escritura			
SignUp	Otorga permiso para registra al usuario en el grupo de usuarios especificado y crea un nombre de usuario, contraseña y atributos de usuario	Escritura			
StartUserImportJob	Concede permiso para iniciar cualquier trabajo de importación de un usuario	Escritura	userpool*		
StopUserImportJob	Concede permiso para detener cualquier trabajo de importación de un usuario	Escritura	userpool*		
TagResource	Concede permiso para etiquetar un grupo de usuarios	Etiquetado	userpool		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar la etiqueta de un grupo de usuarios	Etiquetado	userpool		
				aws:TagKeys	
UpdateAuthEventFeedback	Otorga permiso para actualizar los comentarios del evento de autenticación de usuario	Escritura	userpool*		
UpdateDeviceStatus	Otorga permiso para actualizar el estado del dispositivo	Escritura			
UpdateGroup	Concede permiso para actualizar la configuración de cualquier grupo	Escritura	userpool*		
UpdateIdentityProvider	Concede permiso para actualizar la configuración de cualquier IdP de grupo de usuarios	Escritura	userpool*		
UpdateManagedLoginBranding	Otorga permiso para actualizar la configuración de marca de un inicio de sesión administrado	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateResourceServer	Otorga permiso para actualizar la configuración de cualquier servidor de recursos OAuth 2.0	Escritura	userpool*		
UpdateUserAttributes	Otorga permiso para permitir a un usuario actualizar un atributo específico (uno a la vez)	Escritura			
UpdateUserPool	Concede permiso para actualizar la configuración de grupos de usuarios	Escritura	userpool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateUserPoolClient	Concede permiso para actualizar cualquier cliente de grupos de usuarios	Escritura	userpool*		
UpdateUserPoolDomain	Concede permiso para reemplazar el certificado por cualquier dominio personalizado	Escritura	userpool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
VerifySoftwareToken	Otorga permiso para registrar el código TOTP ingresado del usuario y marca el estado MFA del token de software del usuario como verificado si es correcto	Escritura			
VerifyUserAttribute	Otorga permiso para verificar un atributo de usuario mediante un código de verificación de un solo uso	Escritura			

Tipos de recurso definidos por los grupos de usuarios de Amazon Cognito

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Claves de condición de los grupos de usuarios de Amazon Cognito

Amazon Cognito User Pools define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por una clave que está presente en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para Amazon Comprehend

Amazon Comprehend (prefijo de servicio: `comprehend`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Comprehend
- Tipos de recurso definidos por Amazon Comprehend
- Claves de condición para Amazon Comprehend

Acciones definidas por Amazon Comprehend

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDetectDominantLanguage	Otorga permiso para detectar el idioma o idiomas presentes en la lista de documentos de texto	Read			
BatchDetectEntities	Otorga permiso para detectar las entidades denominadas ("Personas", "Lugares", "Ubicaciones", etc.) dentro de la lista determinada de documentos de texto	Read			
BatchDetectKeyPhrases	Otorga permiso para detectar las frases de la lista de documentos de texto que son las más indicativas del contenido	Read			
BatchDetectSentiment	Otorga permiso para detectar las opiniones de un texto en la lista de documentos (positivo, negativo, neutro o una combinación de estos)	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDetectSyntax	Otorga permiso para detectar información sintáctica (como parte de voz, tokens) en una lista de documentos de texto	Lectura			
BatchDetectTargetedSentiment	Otorga permiso para detectar las opiniones asociadas con entidades específicas (como marcas o productos) dentro de la lista determinada de documentos de texto	Lectura			
ClassifyDocument	Otorga permiso para crear una solicitud de clasificación de documentos nueva para analizar un solo documento en tiempo real, con un modelo personalizado creado y entrenado previamente y con un punto de enlace	Lectura	document-classifier-endpoint*		
ContainsPiiEntities	Otorga permiso para clasificar la información personalmente identificable dentro de los documentos dados en tiempo real	Lectura			
CreateDataset	Concede permiso para crear un nuevo conjunto de datos en un volante de inercia	Escritura	flywheel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocumentClassifier	Otorga permiso para crear un nuevo clasificador de documentos que puede utilizar para categorizar documentos	Write	document-classifier*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEndpoint	Otorga permiso para crear un punto de enlace específico del modelo para la inferencia sincrónica para un modelo personalizado entrenado previamente	Write	document-classifier*		
			document-classifier-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			entity-recognizer*		
			entity-recognizer-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			flywheel		
CreateEntityRecognizer	Otorga permiso para crear un reconocedor de entidades mediante archivos enviados	Escritura	entity-recognizer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFlywheel	Concede permiso para crear un nuevo volante de inercia que se puede utilizar para entrenar versiones de modelos	Escritura	flywheel*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:DataLakeKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDocumentClassifier	Otorga permiso para eliminar un clasificador de documentos creado anteriormente	Write	document-classifier*		
DeleteEndpoint	Otorga permiso para eliminar un punto de enlace específico de un modelo para un modelo personalizado previamente entrenado Para poder eliminar el modelo, se deben borrar todos los puntos de enlace.	Write	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DeleteEntityRecognizer	Otorga permiso para eliminar un reconocedor de entidades enviado	Escritura	entity-recognizer*		
DeleteFlywheel	Concede permiso para eliminar un volante de inercia	Escritura	flywheel*		
DeleteResourcePolicy	Otorga permiso para eliminar la política en el recurso	Escritura	document-classifier*		
			entity-recognizer*		
DescribeDataset	Concede permiso para obtener las propiedades asociadas a un conjunto de datos	Lectura	flywheel-dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDocumentClassificationJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de clasificación de documentos	Read	document-classification-job*		
DescribeDocumentClassifier	Otorga permiso para obtener las propiedades asociadas a un clasificador de documentos	Read	document-classifier*		
DescribeDominantLanguageDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de idioma dominante	Read	dominant-language-detection-job*		
DescribeEndpoint	Otorga permiso para obtener las propiedades asociadas a un punto de enlace específico Utilice esta operación para obtener el estado de un punto de enlace	Read	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DescribeEntitiesDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de entidades	Read	entities-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEntityRecognizer	Otorga permiso para proporcionar información detallada acerca del reconocedor de entidades, incluido estado, buckets de S3 que contienen datos de entrenamiento, metadatos del reconocedor, métricas y así sucesivamente	Read	entity-recognizer*		
DescribeEventsDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de eventos	Lectura	events-detection-job*		
DescribeFlywheel	Concede permiso para obtener las propiedades asociadas a un volante de inercia	Lectura	flywheel*		
DescribeFlywheelIteration	Concede permiso para obtener las propiedades asociadas a una iteración de volante de inercia correspondiente a un volante de inercia	Lectura	flywheel*		
				comprehend:FlywheelIterationId	
DescribeKeyPhrasesDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de frases clave	Read	key-phrases-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePiiEntitiesDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de entidades de PII	Lectura	pii-entities-detection-job*		
DescribeResourcePolicy	Otorga permiso para leer la política adjunta en el recurso	Lectura	document-classifier*		
			entity-recognizer*		
DescribeSentimentDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de opiniones	Lectura	sentiment-detection-job*		
DescribeTargetedSentimentDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de opiniones dirigido	Lectura	targeted-sentiment-detection-job*		
DescribeTopicsDetectionJob	Otorga permiso para obtener las propiedades asociadas a un trabajo de detección de temas	Read	topics-detection-job*		
DetectDominantLanguage	Otorga permiso para detectar el idioma o idiomas presentes en el texto	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetectEntities	Otorga permiso para detectar las entidades nombradas ("Personas", "Lugares", "Ubicaciones", etc.) dentro del documento de texto dado	Read	entity-recognizer-endpoint		
DetectKeyPhrases	Otorga permiso para detectar las frases del texto que son más indicativas del contenido	Read			
DetectPiiEntities	Otorga permiso para detectar las entidades de información de identificación personal ("Nombre", "SSN", "PIN", etc.) dentro del documento de texto dado	Read			
DetectSentiment	Otorga permiso para detectar la opinión de un texto en un documento (Positivo, Negativo, Neutral o Mixto)	Read			
DetectSyntax	Otorga permiso para detectar información sintáctica (como parte de voz, tokens) en un documento de texto	Lectura			
DetectTargetedSentiment	Otorga permiso para detectar las opiniones asociadas con entidades específicas (como marcas o productos) en un documento	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetectToxicContent	Concede permiso para detectar contenido tóxico dentro de la lista de segmentos de texto dada	Lectura			
ImportModel	Otorga permiso para importar un modelo Comprehend entrenado	Escritura	document-classifier*		
			entity-recognizer*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:ModelKmsKey	
ListDatasets	Concede permiso para obtener una lista de los conjuntos de datos asociados a un volante de inercia	Lectura	flywheel*		
ListDocumentClassificationJobs	Otorga permiso para obtener una lista de los trabajos de clasificación de documentos que ha enviado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDocumentClassifierSummaries	Otorga permiso para obtener una lista de resúmenes de los clasificadores de documentos que ha creado	Lectura			
ListDocumentClassifiers	Otorga permiso para obtener una lista de los clasificadores de documentos que ha creado	Lectura			
ListDominantLanguageDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de idiomas dominantes que ha enviado	Lectura			
ListEndpoints	Otorga permiso para obtener una lista de todos los puntos de enlaces existentes que ha creado	Lectura			
ListEntitiesDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de entidades que ha enviado	Lectura			
ListEntityRecognizerSummaries	Otorga permiso para obtener una lista de resúmenes de los reconocedores de entidad que ha creado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntityRecognizers	Otorga permiso para obtener una lista de las propiedades de todos los reconocedores de entidades que ha creado, incluidos reconocedores actualmente en entrenamiento	Lectura			
ListEventsDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de eventos que ha enviado	Lectura			
ListFlywheelIterationHistory	Concede permiso para obtener una lista de iteraciones asociadas correspondientes a un volante de inercia	Lectura	flywheel*		
ListFlywheels	Concede permiso para obtener una lista de los volantes de inercia que se han creado	Lectura			
ListKeyPhrasesDetectionJobs	Otorga permiso para obtener una lista de trabajos de detección de frase clave que ha enviado	Lectura			
ListPiiEntitiesDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de entidades de PII que ha enviado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSentimentDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de opiniones que ha enviado	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTargetedSentimentDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de opiniones dirigidos que ha enviado	Lectura			
ListTopicsDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de temas que ha enviado	Lectura			
PutResourcePolicy	Otorga permiso para adjuntar la política al recurso	Escritura	document-classifier*		
			entity-recognizer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDocumentClassificationJob	Otorga permiso para iniciar un trabajo de clasificación de documentos asíncrono	Write	document-classification-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			flywheel		
StartDominantLanguageDetectionJob	Otorga permiso para iniciar un trabajo de detección de idioma dominante asincrónico para una colección de documentos	Write	dominant-language-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartEntitiesDetectionJob	Otorga permiso para iniciar un trabajo de detección de entidades asincrónicas para una colección de documentos	Write	entities-detection-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			entity-recognizer		
			flywheel		
StartEventsDetectionJob	Otorga permiso para comenzar un trabajo de detección de eventos asíncronos para una colección de documentos	Escritura	events-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartFlywheelIteration	Concede permiso para iniciar una iteración de volante de inercia para un volante de inercia	Escritura	flywheel*		
StartKeyPhrasesDetectionJob	Otorga permiso para iniciar un trabajo de detección de frases clave asincrónicas para una colección de documentos	Write	key-phrases-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartPiiEntitiesDetectionJob	Otorga permiso para iniciar un trabajo de detección de entidades PII asincrónicas para una colección de documentos	Write	pii-entities-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartSentimentDetectionJob	Otorga permiso para iniciar un trabajo de detección de opiniones asincrónica para una colección de documentos	Escritura	sentiment-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTargetedSentimentDetectionJob	Otorga permiso para iniciar un trabajo de detección de opiniones asincrónica dirigida para una colección de documentos	Escritura	targeted-sentiment-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTopicsDetectionJob	Otorga permiso para comenzar una tarea asíncrona para detectar los temas más habituales en la recopilación de documentos y las frases asociadas a cada tema.	Write	topics-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StopDominantLanguageDetectionJob	Otorga permiso para detener un trabajo de detección de idiomas dominante	Write	dominant-language-detection-job*		
StopEntitiesDetectionJob	Otorga permiso para detener un trabajo de detección de entidades	Write	entities-detection-job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopEventsDetectionJob	Otorga permiso para detener un trabajo de detección de eventos	Write	events-detection-job*		
StopKeyPhrasesDetectionJob	Otorga permiso para detener un trabajo de detección de frases clave	Write	key-phrases-detection-job*		
StopPiiEntitiesDetectionJob	Otorga permiso para detener un trabajo de detección de entidades de PII	Write	pii-entities-detection-job*		
StopSentimentDetectionJob	Otorga permiso para detener un trabajo de detección de opiniones	Escritura	sentiment-detection-job*		
StopTargetedSentimentDetectionJob	Otorga permiso para detener un trabajo de detección de opiniones dirigido	Escritura	targeted-sentiment-detection-job*		
StopTrainingDocumentClassifier	Otorga permiso para detener un trabajo de formación de clasificador de documentos creado anteriormente	Write	document-classifier*		
StopTrainingEntityRecognizer	Otorga permiso para detener un trabajo de capacitación de reconocedor de entidades creado anteriormente	Write	entity-recognizer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para desetiquetar un recurso con la clave dada	Etiquetado	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:TagKeys	
UpdateEndpoint	Otorga permiso para actualizar la información sobre el punto de enlace especificado	Escritura	document-classifier-endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			entity-recognizer-endpoint*		
			flywheel		
UpdateFlywheel	Concede permiso para actualizar la configuración de un volante de inercia	Escritura	flywheel*	comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Tipos de recurso definidos por Amazon Comprehend

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
targeted-sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:targeted-sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classifier	arn:${Partition}:comprehend:${Region}:${Account}:document-classifier/${DocumentClassifierName}	aws:ResourceTag/${TagKey}
document-classifier-endpoint	arn:${Partition}:comprehend:${Region}:${Account}:document-classifier-endpoint/${DocumentClassifierEndpointName}	aws:ResourceTag/${TagKey}
entity-recognizer	arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer/${EntityRecognizerName}	aws:ResourceTag/${TagKey}
entity-recognizer-endpoint	arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer-endpoint/${EntityRecognizerEndpointName}	aws:ResourceTag/${TagKey}
dominant-language-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:dominant-language-detection-job/${JobId}	aws:ResourceTag/${TagKey}
entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
pii-entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:pii-entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
events-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:events-detection-job/${JobId}	aws:ResourceTag/${TagKey}
key-phrases-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:key-phrases-detection-job/${JobId}	aws:ResourceTag/${TagKey}
sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
topics-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:topics-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classification-job	arn:${Partition}:comprehend:${Region}:${Account}:document-classification-job/${JobId}	aws:ResourceTag/${TagKey}
flywheel	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}	aws:ResourceTag/${TagKey}
flywheel-dataset	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}/dataset/${DatasetName}	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Comprehend

Amazon Comprehend define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso requiriendo los valores de las etiquetas presentes en una solicitud de creación de recursos	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso requiriendo el valor de la etiqueta asociada al recurso	Cadena
aws:TagKeys	Filtra el acceso requiriendo la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
comprehend:DataLakeKmsKey	Filtra el acceso mediante la clave DataLake Kms asociada al recurso del volante de la solicitud	ARN
comprehend:FlywheelIterationId	Filtra el acceso por ID de iteración particular correspondiente a un volante de inercia	Cadena
comprehend:ModelKmsKey	Filtra el acceso por la clave de KMS del modelo asociado al recurso en la solicitud.	ARN
comprehend:OutputKmsKey	Filtra el acceso por la clave de KMS de salida asociada al recurso en la solicitud.	ARN

Claves de condición	Descripción	Tipo
comprehend:VolumeKmsKey	Filtra el acceso por la clave de KMS del volumen asociada al recurso en la solicitud.	ARN
comprehend:VpcSecurityGroupIds	Filtra el acceso en función de la lista de todos los ID de grupos de seguridad de la VPC asociados al recurso en la solicitud	ArrayOfString
comprehend:VpcSubnets	Filtra el acceso en función de la lista de todas las subredes de la VPC asociadas al recurso en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Comprehend Medical

Amazon Comprehend Medical (prefijo de servicio: `comprehendmedical`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Comprehend Medical
- Tipos de recurso definidos por Amazon Comprehend Medical
- Claves de condición para Amazon Comprehend Medical

Acciones definidas por Amazon Comprehend Medical

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEntitiesDetectionV2Job	Otorga permiso para describir las propiedades de un trabajo de detección de entidad médica que usted ha enviado	Read			
DescribeICD10CMInferenceJob	Otorga permiso para describir las propiedades de un trabajo de vinculación ICD-10-CM que usted ha enviado	Read			
DescribePHIDetectionJob	Otorga permiso para describir las propiedades de un trabajo de detección de entidad PHI que usted ha enviado	Lectura			
DescribeRxNormInferenceJob	Otorga permiso para describir las propiedades de un trabajo de RxNorm enlace que haya enviado	Lectura			
DescribeSNOMEDCTInferenceJob	Otorga permiso para describir las propiedades de un trabajo de vinculación SNOMED-CT que usted ha enviado	Lectura			
DetectEntitiesV2	Otorga permiso para detectar las entidades médicas nombradas, así como sus relaciones y rasgos dentro del documento de texto dado	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetectPHI	Otorga permiso para detectar las entidades de información médica protegida (PHI) dentro del documento de texto dado	Read			
InferICD10CM	Otorga permiso para detectar las entidades de afección médica dentro del documento de texto dado y vincularlas a los códigos ICD-10-CM.	Lectura			
InferRxNorm	Otorga permiso para detectar las entidades farmacológicas dentro del documento de texto en cuestión y vincularlas a los identificadores conceptuales RxCUI de la base de datos de la Biblioteca Nacional de Medicina RxNorm	Lectura			
InferSNOMEDCT	Otorga permiso para detectar la afección médica, la anatomía y las entidades de prueba, tratamiento y procedimiento dentro del documento de texto dado y vincularlos a los códigos SNOMED-CT	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntitiesDetectionV2Jobs	Otorga permiso para obtener una lista de los trabajos de detección de entidades que usted ha enviado	Read			
ListICD10CMInferenceJobs	Otorga permiso para enumerar los trabajos de vinculación ICD-10-CM que usted ha enviado	Read			
ListPHIDetectionJobs	Otorga permiso para obtener una lista de los trabajos de detección de entidades de PHI que usted ha enviado	Lectura			
ListRxNormInferenceJobs	Otorga permiso para enumerar los trabajos de RxNorm enlace que ha enviado	Lectura			
ListSNOMEDCTInferenceJobs	Otorga permiso para enumerar los trabajos de enlace de SNOMED-CT que usted ha enviado	Lectura			
StartEntitiesDetectionV2Job	Otorga permiso para iniciar un trabajo de detección de entidades médicas asincrónicas para una colección de documentos	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartICD10CMInferenceJob	Otorga permiso para comenzar un trabajo de vinculación ICD-10-CM asíncronos para una colección de documentos	Write			
StartPHIDetectionJob	Otorga permiso para iniciar un trabajo de detección de entidades de PHI asincróni cas para un conjunto de documentos	Escritura			
StartRxNormInferenceJob	Otorga permiso para iniciar un trabajo de RxNorm enlace asíncrono para un conjunto de documentos	Escritura			
StartSNOMEDCTInferenceJob	Otorga permiso para iniciar un trabajo de vinculación SNOMED-CT asíncrono para un conjunto de documentos	Escritura			
StopEntitiesDetectionV2Job	Otorga permiso para detener un trabajo de detección de entidades médicas	Write			
StopICD10CMInferenceJob	Otorga permiso para detener un trabajo de vinculación ICD-10-CM	Write			
StopPHIDetectionJob	Otorga permiso para detener un trabajo de detección de entidades de PHI	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopRxNormInferenceJob	Otorga permiso para detener un trabajo de vinculación RxNorm	Escritura			
StopSNOMEDCTInferenceJob	Otorga permiso para detener un trabajo de vinculación SNOMED-CT	Escritura			

Tipos de recurso definidos por Amazon Comprehend Medical

Amazon Comprehend Medical no admite la especificación de un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Amazon Comprehend Medical, especifique `"Resource": "*"` en su política.

Claves de condición para Amazon Comprehend Medical

Amazon Comprehend Medical define las siguientes claves de condición que pueden usarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Compute Optimizer

AWS Compute Optimizer (prefijo de servicio:`compute-optimizer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Compute Optimizer
- Tipos de recursos definidos por AWS Compute Optimizer
- Claves de condición para AWS Compute Optimizer

Acciones definidas por AWS Compute Optimizer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRecommendationPreferences	Otorga permiso para eliminar preferencias de recomendación.	Escritura		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					rds:DescribeDBClusters rds:DescribeDBInstances
DescribeRecommendationExportJobs	Otorga permiso para ver el estado de los trabajos de exportación de recomendaciones.	Enumeración			
ExportAutoScalingGroupRecommendations	Otorga permiso para exportar las recomendaciones de AutoScaling grupo a S3 para las cuentas proporcionadas	Escritura			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExportEBSVolumeRecommendations	Otorga permiso para exportar recomendaciones de volumen de EBS a S3 en las cuentas proporcionadas.	Escritura			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes
ExportEC2InstanceRecommendations	Otorga permiso para exportar las recomendaciones de EC2 instancias a S3 para las cuentas proporcionadas	Escritura			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportECSServiceRecommendations	Concede permiso para exportar recomendaciones de servicios de ECS a S3 para las cuentas proporcionadas	Escritura			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExportIdleRecommendations	Otorga permiso para exportar recomendaciones inactivas a S3 para las cuentas proporcionadas	Escritura			compute-optimizer:GetIdleRecommendations
ExportLambdaFunctionRecommendations	Otorga permiso para exportar recomendaciones de función de Lambda a S3 en las cuentas proporcionadas.	Escritura			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	Concede permiso para exportar recomendaciones de licencias a S3 para las cuentas proporcionadas	Escritura			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExportRDSDatabaseRecommendations	Concede permiso para exportar recomendaciones de RDS a S3 para las cuentas proporcionadas	Escritura			compute-optimizer:GetRDSDatabaseRecommendations rds:DescribeDBClusters rds:DescribeDBInstances
GetAutoScalingGroupRecommendations	Otorga permiso para obtener recomendaciones para los AutoScaling grupos proporcionados	Enumeración			autoscaling:DescribeAutoScalingGroups
GetEBSVolumeRecommendations	Otorga permiso para obtener recomendaciones para los volúmenes EBS proporcionados.	Enumeración			ec2:DescribeVolumes
GetEC2InstanceRecommendations	Otorga permiso para obtener recomendaciones para las EC2 instancias proporcionadas	Enumeración			ec2:DescribeInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEC2RecommendationProjectedMetrics	Otorga permiso para obtener las métricas proyectadas de recomendación de la instancia especificada.	Enumeración			ec2:DescribeInstances
GetECSServiceRecommendationProjectedMetrics	Concede permiso para obtener las métricas proyectadas de recomendación del servicio de ECS especificado	Enumeración			
GetECSServiceRecommendations	Concede permiso para obtener recomendaciones para los servicios de ECS proporcionados	Enumeración			ecs:ListClusters ecs:ListServices

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEffectiveRecommendationPreferences	Otorga permiso para obtener preferencias de recomendación vigentes.	Lectura		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
GetEnrollmentStatus	Otorga permiso para obtener el estado de inscripción de la cuenta especificada.	Enumeración			
GetEnrollmentStatusesForOrganization	Otorga permiso para obtener los estados de inscripción de las cuentas de miembro de la organización	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIdleRecommendations	Otorga permiso para obtener recomendaciones inactivas para las cuentas especificadas	Enumeración			
GetLambdaFunctionRecommendations	Otorga permiso para obtener recomendaciones para las funciones de Lambda proporcionadas.	Enumeración			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	Concede permiso para obtener recomendaciones de licencias para las cuentas especificadas	Enumeración			ec2:DescribeInstances
GetRDSDatabaseRecommendationProjectedMetrics	Otorga permiso para obtener las métricas proyectadas de recomendación de la instancia especificada.	Enumeración			rds:DescribeDBClusters rds:DescribeDBInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRDSDatabaseRecommendations	Concede permiso para obtener recomendaciones de RDS para las cuentas especificadas	Enumeración			rds:DescribeDBClusters rds:DescribeDBInstances
GetRecommendationPreferences	Otorga permiso para obtener preferencias de recomendaciones	Lectura		compute-optimizer:ResourceType	
GetRecommendationSummaries	Otorga permiso para obtener los resúmenes de recomendaciones para las cuentas especificadas.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutRecommendationPreferences	Otorga permiso para colocar preferencias de recomendación.	Escritura		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
UpdateEnrollmentStatus	Otorga permiso para actualizar el estado de inscripción.	Write			

Tipos de recursos definidos por AWS Compute Optimizer

AWS Compute Optimizer no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Compute Optimizer, especifique `"Resource": "*"` en la política.

Claves de condición para AWS Compute Optimizer

AWS Compute Optimizer define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
compute-optimizer:ResourceType	Filtra el acceso por el tipo del recurso.	Cadena

Acciones, recursos y claves de condición para AWS Config

AWS Config (prefijo de servicio:`config`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Config
- Tipos de recursos definidos por AWS Config
- Claves de condición para AWS Config

Acciones definidas por AWS Config

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateResourceTypes	Otorga permiso para agregar todos los tipos de recursos especificados a la grabadora RecordingGroup de configuración e incluye esos tipos de recursos al grabar	Escritura	ConfigurationRecorder*		
BatchGetAggregateResourceConfig	Otorga permiso para devolver los elementos de configuración actuales de los recursos que están presentes en su agregador AWS Config	Lectura	ConfigurationAggregator*		
BatchGetResourceConfig	Otorga permiso para devolver la configuración actual para uno o más recursos solicitados.	Read			
DeleteAggregationAuthorization	Otorga permiso para eliminar la autorización otorgada a la cuenta de agregador de configuración especificada en una región determinada.	Escritura	AggregationAuthorization*		
DeleteConfigRule	Otorga permiso para eliminar la regla de AWS Config especificada y todos sus resultados de evaluación	Escritura	ConfigRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConfigurationAggregator	Otorga permiso para eliminar el agregador de configuración especificado y los datos agregados asociados con el agregador.	Escritura	ConfigurationAggregator*		
DeleteConfigurationRecorder	Otorga permiso para eliminar el grabador de configuración gestionado por el cliente	Escritura	ConfigurationRecorder*		
DeleteConformancePack	Otorga permiso para eliminar el paquete de conformidad especificado y todas las reglas de AWS Config y todos los resultados de evaluación de ese paquete de conformidad	Escritura	ConformancePack*		
DeleteDeliveryChannel	Otorga permiso para eliminar el canal de entrega.	Write			
DeleteEvaluationResults	Otorga permiso para eliminar los resultados de evaluación de la regla de Config especificada.	Write	ConfigRule*		
DeleteOrganizationConfigRule	Otorga permiso para eliminar la regla de Config de organización especificada y todos sus resultados de evaluación de todas las cuentas de miembro de esa organización.	Write	OrganizationConfigRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteOrganizationConformancePack	Otorga permiso para eliminar el paquete especificado de conformidad de la organización y todos sus resultados de evaluación de todas las cuentas de miembro de esa organización.	Write	OrganizationConformancePack*		
DeletePendingAggregationRequest	Otorga permiso para eliminar las solicitudes de autorización pendientes de una cuenta de agregador especificada en una región determinada.	Write			
DeleteRemediationConfiguration	Otorga permiso para eliminar la configuración de corrección.	Escritura	RemediationConfiguration*		
DeleteRemediationExceptions	Otorga permiso para eliminar una o más excepciones de corrección para claves de recursos específicas para una regla de AWS Config específica	Escritura			
DeleteResourceConfig	Otorga permiso para registrar el estado de configuración de un recurso personalizado que se ha eliminado.	Write			
DeleteRetentionConfiguration	Otorga permiso para eliminar la configuración de retención.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteServiceLinkedConfigurationRecorder	Otorga permiso para eliminar el grabador de configuración vinculado al servicio	Escritura	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	Otorga permiso para eliminar la consulta almacenada para un Cuenta de AWS Región de AWS	Escritura	StoredQuery*		
DeliverConfigSnapshot	Otorga permiso para programar la entrega de una instantánea de configuración al bucket de Amazon S3 en el canal de entrega especificado.	Read			
DescribeAggregateComplianceByConfigRules	Otorga permiso para devolver una lista de reglas conformes y no conformes con el número de recursos para las reglas conformes y no conformes.	Read	ConfigurationAggregator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAggregateComplianceByConformancePacks	Otorga permiso para devolver una lista de paquetes de conformidad conformes y no conformes junto con el recuento de reglas conformes, no conformes y totales dentro de cada paquete de conformidad	Read	ConfigurationAggregator*		
DescribeAggregationAuthorizations	Otorga permiso para devolver una lista de autorizaciones otorgadas a varias regiones y cuentas de agregadores.	Enumeración			
DescribeComplianceByConfigRule	Otorga permiso para indicar si las reglas de AWS Config especificadas son compatibles	Lectura			
DescribeComplianceByResource	Otorga permiso para indicar si los AWS recursos especificados son compatibles	Lectura			
DescribeConfigRuleEvaluationStatus	Otorga permiso para devolver la información de estado de cada una de tus reglas de Config AWS gestionadas	Lectura			
DescribeConfigRules	Otorga permiso para devolver detalles sobre tus reglas de AWS Config	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConfigurationAggregatorSourcesStatus	Otorga permiso para devolver información de estado para orígenes dentro de un agregador.	Read	ConfigurationAggregator*		
DescribeConfigurationAggregators	Otorga permiso para devolver los detalles de uno o más agregadores de configuración.	List			
DescribeConfigurationRecorderStatus	Otorga permiso para devolver el estado actual de la grabadora de configuración especificada.	Read	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConfigurationRecorders	Otorga permiso para devolver los nombres de una o más grabadoras de configuración especificadas.	Lectura	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConformancePackCompliance	Otorga permiso para devolver información de conformidad para cada regla de ese paquete de conformidad.	Read	ConformancePack*		
DescribeConformancePackStatus	Otorga permiso para proporcionar uno o más estados de implementación de paquetes de conformidad.	Read			
DescribeConformancePacks	Otorga permiso para devolver una lista de uno o más paquetes de conformidad.	List			
DescribeDeliveryChannelStatus	Otorga permiso para devolver el estado actual del canal de entrega especificado.	Read			
DescribeDeliveryChannels	Otorga permiso para devolver detalles sobre el canal de entrega especificado.	List			
DescribeOrganizationConfigRuleStatuses	Otorga permiso para proporcionar el estado de la implementación de reglas de Config de organización para una organización.	Read			
DescribeOrganizationConfigRules	Otorga permiso para devolver una lista de reglas de Config de la organización.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeOrganizationConformancePackStatuses	Otorga permiso para proporcionar el estado de la implementación del paquete de conformidad de organización de una organización.	Read			
DescribeOrganizationConformancePacks	Otorga permiso para devolver una lista de paquetes de conformidad de organización.	List			
DescribePendingAggregationRequests	Otorga permiso para devolver una lista de todas las solicitudes de agregación pendientes.	List			
DescribeRemediationConfigurations	Otorga permiso para devolver los detalles de una o más configuraciones de corrección.	List	RemediationConfiguration*		
DescribeRemediationExceptions	Otorga permiso para devolver los detalles de una o más excepciones de corrección.	List			
DescribeRemediationExecutionStatus	Otorga permiso para proporcionar una vista detallada de una ejecución de corrección de un conjunto de recursos como estado, marcas de tiempo y cualquier mensaje de error para pasos que han generado un error	Read	RemediationConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRetentionConfigurations	Otorga permiso para devolver los detalles de una o varias configuraciones de retención.	Enumeración			
DisassociateResourceTypes	Otorga permiso para eliminar todos los tipos de recursos especificados RecordingGroup de la grabadora de configuración y excluye estos tipos de recursos al grabar	Escritura	ConfigurationRecorder*		
GetAggregateComplianceDetailsByConfigRule	Otorga permiso para devolver los resultados de la evaluación de la regla AWS Config especificada para un recurso específico en una regla	Lectura	ConfigurationAggregator*		
GetAggregateConfigRuleComplianceSummary	Otorga permiso para devolver el número de reglas conformes y no conformes de una o más cuentas y regiones de un agregador.	Read	ConfigurationAggregator*		
GetAggregateConformancePackComplianceSummary	Otorga permiso para devolver la cantidad de paquetes de conformidad conformes y no conformes de una o más cuentas y regiones en un agregador	Lectura	ConfigurationAggregator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAggregateDiscoveredResourceCounts	Otorga permiso para devolver los recuentos de recursos en todas las cuentas y regiones que están presentes en tu agregador AWS Config	Lectura	ConfigurationAggregator*		
GetAggregateResourceConfig	Otorga permiso para devolver el elemento de configuración que se agrega para su recurso específico en una región y cuenta de origen específicas.	Lectura	ConfigurationAggregator*		
GetComplianceDetailsByConfigRule	Otorga permiso para devolver los resultados de la evaluación de la regla AWS Config especificada	Lectura	ConfigRule*		
GetComplianceDetailsByResource	Otorga permiso para devolver los resultados de la evaluación del AWS recurso especificado	Lectura			
GetComplianceSummaryByConfigRule	Otorga permiso para devolver el número de reglas de AWS Config que cumplen y no lo son, hasta un máximo de 25 por cada una	Lectura			
GetComplianceSummaryByResourceType	Otorga permiso para devolver el número de recursos conformes y el número de no conformes.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConformancePackComplianceDetails	Otorga permiso para devolver los detalles de conformidad de un paquete de conformidad para todos los AWS recursos que supervisa el paquete de conformidad	Lectura	ConformancePack*		
GetConformancePackComplianceSummary	Otorga permiso para proporcionar un resumen de conformidad para uno o más paquetes de conformidad.	Lectura	ConformancePack*		
GetCustomRulePolicy	Otorga permiso para devolver la definición de política que contiene la lógica de la regla AWS Config Custom Policy	Lectura	ConfigRule*		
GetDiscoveredResourceCounts	Otorga permiso para devolver los tipos de recursos, el número de cada tipo de recurso y el número total de recursos que AWS Config registra en esta región para su Cuenta de AWS	Lectura			
GetOrganizationConfigRuleDetailedStatus	Otorga permiso para devolver el estado detallado de cada cuenta de miembro dentro de una organización para una regla de Config de organización determinada.	Read	OrganizationConfigRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOrganizationConformancePackDetailedStatus	Otorga permiso para devolver el estado detallado de cada cuenta de miembro dentro de una organización para un paquete de conformidad de organización determinado.	Lectura	OrganizationConformancePack*		
GetOrganizationCustomRulePolicy	Otorga permiso para devolver la definición de política que contiene la lógica de la regla AWS Config Custom Policy de su organización	Lectura	OrganizationConfigRule*		
GetResourceConfigHistory	Otorga permiso para devolver una lista de elementos de configuración para el recurso especificado.	Lectura			
GetResourceEvaluationSummary	Concede permiso para devolver el resumen de evaluaciones de recursos para un ID de evaluación de recursos específico	Lectura			
GetStoredQuery	Otorga permiso para devolver los detalles de una consulta almacenada específica.	Read	StoredQuery*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAggregateDiscoveredResources	Otorga permiso para aceptar un tipo de recurso y devuelve una lista de los identificadores de recursos que se agregan para un tipo de recurso específico entre las cuentas y las regiones.	Enumeración	ConfigurationAggregator*		
ListConfigurationRecorders	Otorga permiso para enumerar los resúmenes de los registradores de configuración de un Cuenta de AWS en un Región de AWS	Enumeración			
ListConformancePackComplianceScores	Otorga permiso para devolver el porcentaje de combinaciones de reglas y recursos conformes en un paquete de conformidad en comparación con el número total de combinaciones posibles de reglas y recursos	Enumeración			
ListDiscoveredResources	Otorga permiso para aceptar un tipo de recurso y devuelve una lista de los identificadores de recursos para los recursos de ese tipo.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourceEvaluations	Otorga permiso para enumerar los resúmenes de evaluación de recursos de un en un Cuenta de AWS Región de AWS	Enumeración			
ListStoredQueries	Otorga permiso para enumerar las consultas almacenadas de un Cuenta de AWS en un Región de AWS	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso AWS Config	Lectura	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			OrganizationConformancePack		
			StoredQuery		
PutAggregationAuthorization	Otorga permiso para autorizar a la cuenta y la región del agregador a que recopilen datos de la cuenta y la región de origen.	Escritura	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	Otorga permiso para agregar o actualizar una regla de AWS Config para evaluar si sus AWS recursos cumplen con las configuraciones deseadas	Escritura	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConfigurationAggregator	Otorga permiso para crear y actualizar el agregador de configuración con las cuentas y las regiones de origen seleccionadas.	Escritura	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	Otorga permiso para crear o actualizar un grabador de configuración administrado por el cliente para registrar las configuraciones de recursos seleccionadas	Escritura	ConfigurationRecorder*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConformancePack	Otorga permiso para crear o actualizar un paquete de conformidad.	Write	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument
PutDeliveryChannel	Otorga permiso para crear un objeto de canal de entrega para enviar información de configuración a un bucket de Amazon S3 y un tema de Amazon SNS.	Escritura			
PutEvaluations	Otorga permiso para que una función AWS Lambda la utilice para entregar los resultados de la evaluación a Config AWS	Escritura			
PutExternalEvaluation	Otorga permiso para entregar el resultado de la evaluación a AWS Config	Escritura	ConfigRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutOrganizationConfigRule	Otorga permiso para agregar o actualizar la regla de configuración de la organización para toda la organización, evaluando si sus AWS recursos cumplen con las configuraciones deseadas	Escritura	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutOrganizationConformancePack	Otorga permiso para añadir o actualizar el paquete de conformidad organizacional para toda la organización, evaluando si AWS los recursos cumplen con las configuraciones deseadas	Escritura	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	Otorga permiso para añadir o actualizar la configuración de corrección con una regla de AWS Config específica con el objetivo o la acción seleccionados	Escritura	RemediationConfiguration*		iam:PassRole
PutRemediationExceptions	Otorga permiso para agregar o actualizar excepciones de corrección para recursos específicos para una regla de AWS Config específica	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResourceConfig	Otorga permiso para registrar el estado de configuración del recurso proporcionado en la solicitud.	Escritura			
PutRetentionConfiguration	Otorga permiso para crear y actualizar la configuración de retención con detalles sobre el período de retención (número de días) durante el que AWS Config almacena su información histórica	Escritura			
PutServiceLinkedConfigurationRecorder	Otorga permiso para crear un nuevo registrador de configuraciones vinculadas al servicio para registrar las configuraciones de recursos incluidas en el ámbito del servicio vinculado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys config:ConfigurationRecorderServicePrincipal	iam:CreateServiceLinkedRole iam:PassRole
PutStoredQuery	Otorga permiso para guardar una nueva consulta o actualiza una consulta guardada existente.	Escritura	StoredQuery*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
SelectAggregateResourceConfig	Otorga permiso para aceptar un comando SELECT de lenguaje de consultas estructurado (SQL) y un agregador para consultar el estado de configuración de AWS los recursos en varias cuentas y regiones, realiza la búsqueda correspondiente y devuelve las configuraciones de los recursos que coinciden con las propiedades	Lectura	ConfigurationAggregator*		
SelectResourceConfig	Otorga permiso para aceptar un comando SELECT de lenguaje de consulta estructurada (SQL); realiza la búsqueda correspondiente y devuelve las configuraciones de recursos de las propiedades coincidentes.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartConfigRulesEvaluation	Otorga permiso para evaluar sus recursos con respecto a las reglas de Config especificadas.	Escritura	ConfigRule*		
StartConfigurationRecorder	Concede permiso al grabador de configuración gestionado por el cliente para que comience a grabar las configuraciones de los AWS recursos que ha seleccionado para grabarlas en su Cuenta de AWS	Escritura	ConfigurationRecorder*		
StartRemediationExecution	Otorga permiso para ejecutar una corrección bajo demanda para las reglas de AWS Config especificadas en función de la última configuración de corrección conocida	Escritura			iam:PassRole
StartResourceEvaluation	Otorga permiso para evaluar los detalles de tus recursos según las reglas de AWS Config de tu cuenta	Escritura			cloudformation:DescribeType

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopConfigurationRecorder	Concede permiso al grabador de configuración gestionado por el cliente para que deje de grabar las configuraciones de AWS los recursos que ha seleccionado para grabarlas en su Cuenta de AWS	Escritura	ConfigurationRecorder*		
TagResource	Otorga permiso para asociar las etiquetas especificadas a un recurso con el ARN de recurso especificado.	Etiquetado	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar las etiquetas especificadas de un recurso.	Etiquetado	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

Tipos de recursos definidos por AWS Config

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AggregationAuthorization	`arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}`	aws:ResourceTag/${TagKey}
ConfigurationAggregator	`arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
ConfigRule	arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}	aws:ResourceTag/${TagKey}
ConformancePack	arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}	aws:ResourceTag/${TagKey}
OrganizationConfigRule	arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}	aws:ResourceTag/${TagKey}
OrganizationConformancePack	arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}	aws:ResourceTag/${TagKey}
RemediationConfiguration	arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}
ConfigurationRecorder	arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Config

AWS Config define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
config:ConfigurationRecorderServicePrincipal	Filtra el acceso por principal de servicio del registrador de configuración	Cadena

Acciones, recursos y claves de condición para Amazon Connect Cases

Amazon Connect Cases (prefijo de servicio: `cases`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Connect Cases
- Tipos de recurso definidos por Amazon Connect Cases

- Claves de condición de Amazon Connect Cases

Acciones definidas por Amazon Connect Cases

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetCaseRule	Otorga permiso para recuperar información sobre las reglas del caso en el dominio del caso	Lectura	CaseRule*		
			Domain*		
BatchGetField	Concede permiso para recuperar información sobre los campos en el dominio de casos	Lectura	Domain*		
			Field*		
BatchPutFieldOptions	Concede permiso para actualizar las opciones de campo en el dominio de casos	Escritura	Domain*		
			Field*		
CreateCase	Concede permiso para crear un caso en el dominio de casos	Escritura	Case*		
			Domain*		
			Field*		
			Template*		
				connect:UserArn	
CreateCaseRule		Escritura	CaseRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para crear una regla de casos en el dominio de casos		Domain*		
CreateDomain	Concede permiso para crear un nuevo dominio de casos	Escritura			
CreateField	Concede permiso para crear un campo en el dominio de casos	Escritura	Domain*		
			Field*		
CreateLayout	Concede permiso para crear un diseño en el dominio de casos	Escritura	Domain*		
			Layout*		
CreateRelatedItem	Concede permiso para crear un elemento relacionado asociado a un caso en el dominio de casos	Escritura	Case*		
			Domain*		
			RelatedItem*		
				connect:UserArn	
CreateTemplate	Concede permiso para crear una plantilla en el dominio de casos	Escritura	Domain*		
			Layout*		
			Template*		
DeleteCaseRule	Otorga permiso para eliminar la regla de casos en el dominio de casos	Escritura	CaseRule*		
			Domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDomain	Concede permiso para eliminar el dominio	Escritura	Domain*		
DeleteField	Concede permiso para eliminar el campo en el dominio de casos	Escritura	Domain*		
			Field*		
DeleteLayout	Concede permiso para eliminar el diseño en el dominio de casos	Escritura	Domain*		
			Layout*		
DeleteRelatedItem [solo permiso]	Concede permiso para eliminar un elemento relacionado asociado a un caso en el dominio de casos	Escritura	Case*		
			Domain*		
			RelatedItem*		
DeleteTemplate	Concede permiso para eliminar la plantilla en el dominio de casos	Escritura	Domain*		
			Template*		
GetCase	Concede permiso para recuperar información sobre un caso en el dominio de casos	Lectura	Case*		
			Domain*		
			Field*		
GetCaseAuditEvents	Concede permiso para ver el historial de auditoría de un caso	Lectura	Case*		
			Domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCaseEventConfiguration	Concede permiso para recuperar información acerca de la configuración de eventos de caso en el dominio de casos	Lectura	Domain*		
GetDomain	Concede permiso para recuperar información acerca del dominio de casos	Lectura	Domain*		
GetLayout	Concede permiso para recuperar información acerca del diseño en el dominio de casos	Lectura	Domain*		
			Layout*		
GetTemplate	Concede permiso para recuperar información acerca de la plantilla en el dominio de casos	Lectura	Domain*		
			Template*		
ListCaseRules	Otorga permiso para enumerar las reglas de casos en el dominio de casos	Enumeración	Domain*		
ListCasesForContact	Concede permiso para enumerar casos para un contacto específico en el dominio de casos	Enumeración	Domain*		
ListDomains	Otorga permiso para enumerar todos los dominios en la cuenta de aws	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFieldOptions	Concede permiso para enumerar las opciones de campo para un solo campo de selección en el dominio de casos	Enumeración	Domain* Field*		
ListFields	Concede permiso para enumerar los campos en el dominio de casos	Enumeración	Domain*		
ListLayouts	Otorga permiso para enumerar diseños en el dominio de casos	Enumeración	Domain*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso especificado	Lectura			
ListTemplates	Concede permiso para enumerar las plantillas en el dominio de casos	Enumeración	Domain*		
PutCaseEventConfiguration	Concede permiso para insertar o actualizar la configuración de eventos de casos en el dominio de casos	Escritura	Domain*		
SearchCases	Concede permiso para buscar casos en el dominio de casos	Lectura	Domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchRelatedItems	Concede permiso para buscar elementos relacionados asociados al caso en el dominio de casos	Lectura	Case*		
			Domain*		
TagResource	Otorga permiso para agregar las etiquetas especificadas al recurso especificado	Etiquetado	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para quitar las etiquetas especificadas de los recursos especificados	Etiquetado	Case		
			CaseRule		
			Domain		
			Field		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Layout		
			RelatedItem		
			Template		
				aws:TagKeys	
UpdateCase	Concede permiso para actualizar los valores de campo del caso en el dominio de casos	Escritura	Case*		
			Domain*		
			Field*		
				connect:UserArn	
UpdateCaseRule	Otorga permiso para actualizar la regla de casos en el dominio de casos	Escritura	CaseRule*		
			Domain*		
UpdateField	Concede permiso para actualizar el campo en el dominio de casos	Escritura	Domain*		
			Field*		
UpdateLayout	Concede permiso para actualizar el diseño en el dominio de casos	Escritura	Domain*		
			Layout*		
UpdateTemplate	Concede permiso para actualizar la plantilla en el dominio de casos	Escritura	Domain*		
			Template*		

Tipos de recurso definidos por Amazon Connect Cases

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Case	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}`	aws:ResourceTag/${TagKey}
Domain	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}
Field	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/field/${FieldId}`	aws:ResourceTag/${TagKey}
Layout	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/layout/${LayoutId}`	aws:ResourceTag/${TagKey}
RelatedItem	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}/related-item/${RelatedItemId}`	aws:ResourceTag/${TagKey}
Template	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}
CaseRule	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case-rule/${CaseRuleId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Connect Cases

Amazon Connect Cases define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
connect:UserArn	Filtra el acceso por conexión UserArn	ARN

Acciones, recursos y claves de condición para Amazon Connect Customer Profiles

Amazon Connect Customer Profiles (prefijo de servicio: `profile`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Connect Customer Profiles
- Tipos de recursos definidos por Amazon Connect Customer Profiles
- Claves de condición de Amazon Connect Customer Profiles

Acciones definidas por Amazon Connect Customer Profiles

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddProfileKey	Otorga permiso para agregar una clave de perfil	Escritura	domains*		
BatchGetCalculatedAttributeForProfile	Concede permiso para recuperar un atributo calculado para los perfiles específicos del dominio	Lectura	calculated-attributes*		
			domains*		
BatchGetProfile	Concede permiso para obtener perfiles en el dominio	Lectura	domains*		
CreateCalculatedAttributeDefinition	Concede permiso para crear una definición de atributo calculada en el dominio	Escritura	calculated-attributes*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDomain	Otorga permiso para crear un dominio	Escritura	domains*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateDomainLayout	Otorga permiso para crear un diseño en el dominio	Escritura	domains*		
			layouts*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventStream	Concede permiso para mostrar un flujo de eventos en un dominio	Escritura	domains*		iam:PutRolePolicy kinesis:DescribeStreamSummary
			event-streams*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventTrigger	Otorga permiso para crear un activador de eventos en el dominio	Escritura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			event-triggers*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationWorkflow	Otorga permiso para crear un flujo de trabajo de integración en un dominio	Escritura	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Otorga permiso para crear un perfil en el dominio	Escritura	domains*		
CreateSegmentDefinition	Concede permiso para crear una definición de segmento en el dominio	Escritura	domains*		
			segment-definitions*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentEstimate	Concede permiso para crear una estimación de segmento en el dominio	Escritura	domains*		
CreateSegmentSnapshot	Concede permiso para crear una instantánea de segmento en el dominio	Escritura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			segment-definitions*		
CreateSnapshot [solo permiso]	Concede permiso para crear una instantánea en el dominio	Escritura	domains*		
CreateUploadJob	Otorga permiso para crear un trabajo de carga en el dominio	Escritura	domains*		
DeleteCalculatedAttributeDefinition	Concede permiso para eliminar una definición de atributo calculada del dominio	Escritura	calculated-attributes*		
			domains*		
DeleteDomain	Da permiso para eliminar un dominio.	Escritura	domains*		
DeleteDomainLayout	Otorga permiso para eliminar un diseño en el dominio	Escritura	domains*		
			layouts*		
DeleteEventStream	Concede permiso para eliminar un flujo de eventos de un dominio	Escritura	domains*		iam:DeleteRolePolicy
			event-streams*		
DeleteEventTrigger	Otorga permiso para eliminar un desencadenador de eventos en el dominio	Escritura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			event-triggers*		
DeleteIntegration	Otorga permiso para eliminar una integración en un dominio	Write	domains*		
			integrations*		
DeleteProfile	Concede permiso para eliminar un perfil	Write	domains*		
DeleteProfileKey	Otorga permiso para eliminar una clave de perfil	Write	domains*		
DeleteProfileObject	Otorga permiso para eliminar un objeto de perfil	Write	domains*		
			object-types*		
DeleteProfileObjectType	Otorga permiso para eliminar un tipo específico de objeto de perfil del dominio	Escritura	domains*		
			object-types*		
DeleteSegmentDefinition	Concede permiso para eliminar una definición de segmento en el dominio	Escritura	domains*		
			segment-definitions*		
DeleteWorkflow	Otorga permiso para eliminar un flujo de trabajo de integración en un dominio	Escritura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetectProfileObjectType	Concede permisos para detectar automáticamente el tipo de objeto	Lectura	domains*		
GetAutoMergingPreview	Otorga permiso para obtener una vista previa de la combinación automática en un dominio.	Lectura	domains*		
GetCalculatedAttributeDefinition	Concede permiso para obtener una definición de atributo calculada en el dominio	Lectura	calculated-attributes*		
			domains*		
GetCalculatedAttributeForProfile	Concede permiso para recuperar un atributo calculado para un perfil específico del dominio	Lectura	calculated-attributes*		
			domains*		
GetDomain	Otorga permiso para obtener un dominio específico en una cuenta	Lectura	domains*		
GetDomainLayout	Otorga permiso para obtener un diseño en el dominio	Lectura	domains*		
			layouts*		
GetEventStream	Concede permiso para obtener un flujo de eventos específico en un dominio	Lectura	domains*		kinesis:DescribeStreamSummary

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			event-streams*		
GetEventTrigger	Otorga permiso para incluir un activador de eventos en el dominio	Lectura	domains*		
			event-triggers*		
GetIdentityResolutionJob	Otorga permisos para obtener un trabajo de resolución de identidad en un dominio.	Lectura	domains*		
GetIntegration	Otorga permiso para obtener integraciones específicas en un dominio	Lectura	domains*		
			integrations*		
GetMatches	Otorga permisos para obtener coincidencias de perfil en un dominio.	Enumeración	domains*		
GetProfileObjectType	Otorga permiso para obtener un tipo específico de objeto de perfil en el dominio	Read	domains*		
			object-types*		
GetProfileObjectTypeTemplate	Otorga permiso para obtener una plantilla específica de tipo de objeto	Lectura			
GetSegmentDefinition	Concede permiso para obtener una definición de segmento en el dominio	Lectura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			segment-definitions*		
GetSegmentEstimate	Concede permiso para obtener una estimación de segmento en el dominio	Lectura	domains*		
GetSegmentMembership	Concede permiso para determinar si los perfiles dados forman parte de un segmento en el dominio	Lectura	domains*		
			segment-definitions*		
GetSegmentSnapshot	Concede permiso para obtener una instantánea de segmento en el dominio	Lectura	domains*		
			segment-definitions*		
GetSimilarProfiles	Otorga permiso para obtener todos los perfiles similares en el dominio	Enumeración	domains*		
GetSnapshot [solo permiso]	Concede permiso para obtener una instantánea en el dominio	Lectura	domains*		
GetUploadJob	Otorga permiso para obtener detalles de un trabajo de carga en el dominio	Lectura	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetUploadJobPath	Otorga permiso para obtener una URL prefirmada para cargar un archivo para un trabajo de carga	Lectura	domains*		
GetWorkflow	Otorga permisos para obtener detalles de flujo de trabajo en un dominio	Lectura	domains*		
GetWorkflowSteps	Otorga permisos para obtener detalles de pasos de flujo de trabajo en un dominio	Lectura	domains*		
ListAccountIntegrations	Otorga permiso para obtener una lista de todas las integraciones de la cuenta	Enumeración			
ListCalculatedAttributeDefinitions	Concede permiso para obtener una lista de todas las definiciones de atributos calculadas en el dominio	Enumeración	domains*		
ListCalculatedAttributesForProfile	Concede permiso para enumerar todos los atributos calculados de un perfil específico en el dominio	Enumeración	domains*		
ListDomainLayouts	Otorga permiso para enumerar todos los diseños del dominio	Enumeración	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDomains	Otorga permiso para obtener una lista de todos los dominios de una cuenta.	Enumeración			
ListEventStreams	Concede permiso para enumerar todos los flujos de eventos en un dominio específico	Enumeración	domains*		
ListEventTriggers	Otorga permiso para enumerar todos los activadores de eventos del dominio	Enumeración	domains*		
ListIdentityResolutionJobs	Otorga permisos para enumerar los trabajos de resolución de identidad en un dominio.	Enumeración	domains*		
ListIntegrations	Otorga permiso para obtener una lista de todas las integraciones de un dominio específico	Enumeración	domains*		
ListObjectTypeAttributes	Concede permiso para enumerar todos los atributos de un tipo de objeto específico en el dominio	Enumeración	domains* object-types*		
ListProfileAttributeValues	Otorga permiso para enumerar todos los valores de un atributo de perfil en el dominio	Enumeración	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProfileObjectTypeTemplates	Otorga permiso para obtener una lista de todas las plantillas de tipo de objeto de perfil de la cuenta	List			
ListProfileObjectTypes	Otorga permiso para obtener una lista de todos los tipos de objetos de perfil del dominio	List	domains*		
ListProfileObjects	Otorga permiso para obtener una lista de todos los objetos de un perfil	Enumeración	domains*		
			object-types*		
ListRuleBasedMatches	Otorga permiso para enumerar todos los resultados coincidentes basados en reglas en el dominio	Enumeración	domains*		
ListSegmentDefinitions	Concede permiso para enumerar todas las definiciones de segmento en el dominio	Enumeración	domains*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	calculated-attributes		
			domains		
			event-streams		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			event-triggers		
			integrations		
			layouts		
			object-types		
			segment-definitions		
ListUploadJobs	Otorga permiso para enumerar todos los trabajos de carga del dominio	Enumeración	domains*		
ListWorkflows	Otorga permiso para listar de todos los flujos de trabajo en un dominio específico	Enumeración	domains*		
MergeProfiles	Concede permiso para combinar perfiles en un dominio	Escritura	domains*		
PutIntegration	Otorga permiso para colocar una integración en un dominio	Write	domains*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
PutProfileObject	Otorga permiso para colocar un objeto de un perfil	Write	domains*		
			object-types*		
PutProfileObjectType	Otorga permiso para colocar un tipo específico de objeto de perfil en el dominio	Write	domains*		
			object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
SearchProfiles	Otorga permiso para buscar perfiles en un dominio	Lectura	domains*		
StartUploadJob	Otorga permiso para iniciar un trabajo de carga en el dominio	Escritura	domains*		
StopUploadJob	Otorga permiso para detener un trabajo de carga en el dominio	Escritura	domains*		
TagResource	Concede permiso para agregar etiquetas a un recurso	Etiquetado	calculated-attributes		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			segment-definitions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	calculated-attributes		
			domains		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			segment-definitions		
				aws:TagKeys	
UpdateCalculatedAttributeDefinition	Concede permiso para actualizar una definición de atributo calculada en el dominio	Escritura	calculated-attributes*		
			domains*		
UpdateDomain	Concede permiso para actualizar un dominio	Escritura	domains*		iam:CreateServiceLinkedRole
UpdateDomainLayout	Otorga permiso para actualizar un diseño en el dominio	Escritura	domains*		
			layouts*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEventTrigger	Otorga permiso para actualizar un desencadenador de eventos en el dominio	Escritura	domains*		
			event-triggers*		
UpdateProfile	Otorga permiso para actualizar un perfil en el dominio	Write	domains*		

Tipos de recursos definidos por Amazon Connect Customer Profiles

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
domains	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}`	aws:ResourceTag/${TagKey}
object-types	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/object-types/${ObjectTypeName}`	aws:ResourceTag/${TagKey}
integrations	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/integrations/${Uri}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
event-streams	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-streams/${EventStreamName}`	aws:ResourceTag/${TagKey}
calculated-attributes	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/calculated-attributes/${CalculatedAttributeName}`	aws:ResourceTag/${TagKey}
segment-definitions	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/segment-definitions/${SegmentDefinitionName}`	aws:ResourceTag/${TagKey}
event-triggers	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-triggers/${EventTriggerName}`	aws:ResourceTag/${TagKey}
layouts	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/layouts/${LayoutDefinitionName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Connect Customer Profiles

Los perfiles de clientes de Amazon Connect definen las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por una clave que está presente en la solicitud que el usuario realiza al servicio de perfil de clientes	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena
aws:TagKeys	Filtra el acceso por la lista de todos los nombres de clave de etiqueta presentes en la solicitud que el usuario realiza al servicio de perfil de clientes	ArrayOfString

Acciones, recursos y claves de condición de las campañas salientes de Amazon Connect

Amazon Connect Outbound Campaigns (prefijo de servicio:`connect-campaigns`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las campañas salientes de Amazon Connect
- Tipos de recursos definidos por las campañas salientes de Amazon Connect
- Claves de condición de las campañas salientes de Amazon Connect

Acciones definidas por las campañas salientes de Amazon Connect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCampaign	Otorga permiso para crear una campaña	Escritura	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCampaign	Otorga permiso para eliminar una campaña	Escritura	campaign*		
DeleteCampaignChannelSubtypeConfig	Otorga permiso para eliminar la configuración de subtipos de canal de una campaña	Escritura	campaign*		
DeleteCampaignCommunicationLimits	Otorga permiso para eliminar la configuración de límites de comunicación de una campaña	Escritura	campaign*		
DeleteCampaignCommunicationTime	Otorga permiso para eliminar la configuración de tiempo de comunicación de una campaña	Escritura	campaign*		
DeleteConnectInstanceConfig	Otorga permiso para eliminar información de configuración	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de una instancia de Amazon Connect				
DeleteConnectInstanceIntegration	Otorga permiso para eliminar la información de integración de una instancia de Amazon Connect	Escritura			
DeleteInstanceOnboardingJob	Otorga permisos para eliminar trabajos de incorporación de una instancia de Amazon Connect	Escritura			
DescribeCampaign	Otorga permiso para describir una campaña específica	Lectura	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignState	Otorga permiso para obtener el estado de una campaña	Lectura	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignStateBatch	Otorga permiso para obtener el estado de una campaña	Lectura	campaign*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnectInstanceConfig	Otorga permiso para obtener información de configuración de una instancia de Amazon Connect	Lectura			
GetInstanceCommunicationLimits	Otorga permiso para obtener la configuración de límites de comunicación de una instancia de Amazon Connect	Lectura			
GetInstanceOnboardingJobStatus	Otorga permisos para obtener el estado de trabajos de incorporación de una instancia de Amazon Connect	Lectura			
ListCampaigns	Otorga permiso para proporcionar un resumen de todas las campañas	Enumeración		aws:RequestTag/${TagKey}	
ListConnectInstanceIntegrations	Otorga permiso para proporcionar un resumen de todas las integraciones con una instancia de Amazon Connect	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	campaign		
				aws:ResourceTag/${TagKey}	
PauseCampaign	Otorga permiso para pausar una campaña	Escritura	campaign*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConnectInstanceIntegration	Otorga permiso para colocar una configuración de integración con una instancia de Amazon Connect	Escritura			
PutDialRequestBatch	Otorga permiso para crear solicitudes de marcado para la campaña especificada	Escritura	campaign*		
PutInstanceCommunicationLimits	Otorga permiso para poner la configuración de límites de comunicación de una instancia de Amazon Connect	Escritura			
PutOutboundRequestBatch	Otorga permiso para crear solicitudes de marcado para la campaña especificada	Escritura	campaign*		
PutProfileOutboundRequestBatch	Otorga permiso para crear solicitudes salientes de perfil para la campaña especificada	Escritura	campaign*		
ResumeCampaign	Otorga permiso para resumir una campaña	Escritura	campaign*		
StartCampaign	Otorga permiso para comenzar una campaña	Escritura	campaign*		
StartInstanceOnboardingJob	Otorga permisos para iniciar trabajos de incorporación para una instancia de Amazon Connect	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopCampaign	Otorga permiso para detener una campaña	Escritura	campaign*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	campaign*		
				aws:TagKeys	
UpdateCampaignChannelSubtypeConfig	Otorga permiso para actualizar la configuración de subtipos de canal de una campaña	Escritura	campaign*		
UpdateCampaignCommunicationLimits	Otorga permiso para actualizar la configuración de los límites de comunicación de una campaña	Escritura	campaign*		
UpdateCampaignCommunicationTime	Otorga permiso para actualizar la configuración del tiempo de comunicación de una campaña	Escritura	campaign*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCampaignDialerConfig	Otorga permiso para actualizar la configuración del marcador de una campaña	Escritura	campaign*		
UpdateCampaignFlowAssociation	Otorga permiso para actualizar la asociación de flujos de una campaña	Escritura	campaign*		
UpdateCampaignName	Otorga permiso para actualizar el nombre de una campaña	Escritura	campaign*		
UpdateCampaignOutboundCallConfig	Otorga permiso para actualizar la configuración de la llamada saliente de una campaña	Escritura	campaign*		
UpdateCampaignSchedule	Otorga permiso para actualizar la programación de una campaña	Escritura	campaign*		
UpdateCampaignSource	Otorga permiso para actualizar la fuente de una campaña	Escritura	campaign*		

Tipos de recursos definidos por las campañas salientes de Amazon Connect

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
campaign	`arn:${Partition}:connect-campaigns:${Region}:${Account}:campaign/${CampaignId}`	aws:ResourceTag/${TagKey}

Claves de condición de las campañas salientes de Amazon Connect

Amazon Connect Outbound Campaigns define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante acciones en función de pares de clave-valor asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante acciones en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Connect Voice ID

Amazon Connect Voice ID (prefijo de servicio: `voiceid`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Connect Voice ID
- Tipos de recurso definidos por Amazon Connect Voice ID
- Claves de condición de Amazon Connect Voice ID

Acciones definidas por Amazon Connect Voice ID

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateFraudster	Concede permiso para asociar a un estafador a una lista de vigilancia	Escritura	domain*		
CreateDomain	Concede permiso para crear un dominio	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWatchlist	Concede permiso para crear una lista de vigilancia	Escritura	domain*		
DeleteDomain	Concede permiso para eliminar un dominio	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFraudster	Concede permiso para eliminar a un estafador	Escritura	domain*		
DeleteSpeaker	Concede permiso para eliminar un locutor	Escritura	domain*		
DeleteWatchlist	Concede permiso para eliminar una lista de vigilancia	Escritura	domain*		
DescribeComplianceConsent [solo permiso]	Concede permiso para describir el consentimiento de conformidad	Lectura			
DescribeDomain	Concede permiso para describir un dominio	Lectura	domain*		
DescribeFraudster	Concede permiso para describir un estafador	Lectura	domain*		
DescribeFraudsterRegistrationJob	Concede permiso para describir el trabajo de registro de un estafador	Lectura	domain*		
DescribeSpeaker	Concede permiso para describir un locutor	Lectura	domain*		
DescribeSpeakerEnrollmentJob	Concede permiso para describir el trabajo de inscripción de un locutor	Lectura	domain*		
DescribeWatchlist	Concede permiso para describir una lista de vigilancia	Lectura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateFraudster	Concede permiso para desasociar a un estafador de una lista de vigilancia	Escritura	domain*		
EvaluateSession	Concede permiso para evaluar una sesión	Escritura	domain*		
ListDomains	Concede permiso para enumerar los dominios de una cuenta	Enumeración			
ListFraudsterRegistrationJobs	Concede permiso para enumerar trabajos de registro de estafadores para un dominio	Enumeración	domain*		
ListFraudsters	Concede permiso para enumerar estafadores de un dominio o una lista de vigilancia	Enumeración	domain*		
ListSpeakerEnrollmentJobs	Concede permiso para enumerar trabajos de inscripción de locutores para un dominio	Enumeración	domain*		
ListSpeakers	Concede permiso para enumerar locutores para un dominio	Enumeración	domain*		
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso Voice ID	Lectura	domain		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWatchlists	Concede permiso para enumerar las listas de vigilancia de un dominio	Enumeración	domain*		
OptOutSpeaker	Concede permiso para inhabilitar un locutor	Escritura	domain*		
RegisterComplianceConsent [solo permiso]	Concede permiso para registrar el consentimiento de conformidad	Escritura			
StartFraudsterRegistrationJob	Concede permiso para comenzar un trabajo de registro de un estafador	Escritura	domain*		
StartSpeakerEnrollmentJob	Concede permiso para comenzar un trabajo de inscripción de un locutor	Escritura	domain*		
TagResource	Concede permiso para etiquetar un recurso Voice ID	Etiquetado	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para quitar una etiqueta de un recurso Voice ID	Etiquetado	domain		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDomain	Concede permiso para actualizar un dominio	Escritura	domain*		
UpdateWatchlist	Concede permiso para actualizar una lista de vigilancia	Escritura	domain*		

Tipos de recurso definidos por Amazon Connect Voice ID

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:voiceid:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Connect Voice ID

Amazon Connect Voice ID define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Connector Service

AWS Connector Service (prefijo de servicio:`awsconnector`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Connector Service
- Tipos de recursos definidos por AWS Connector Service
- Claves de condición para AWS Connector Service

Acciones definidas por AWS Connector Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnectorHealth [solo permiso]	Recupera todas las métricas de mantenimiento publicadas desde el Conector de migración del servidores.	Read			
RegisterConnector [solo permiso]	Registra el AWS conector con el servicio AWS Connector.	Escritura			
ValidateConnectorId [solo permiso]	Valida el identificador del conector de migración del servidor registrado en el servicio AWS Connector.	Lectura			

Tipos de recursos definidos por AWS Connector Service

AWS El servicio Connector no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Connector Service, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Connector Service

Connector Service no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Aplicación móvil de AWS Management Console

AWS Management Console La aplicación móvil (prefijo de servicio:`consoleapp`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Aplicación móvil de AWS Management Console
- Tipos de recursos definidos por Aplicación móvil de AWS Management Console
- Claves de condición para Aplicación móvil de AWS Management Console

Acciones definidas por Aplicación móvil de AWS Management Console

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeviceIdentity	Otorga permiso para recuperar la identidad de un dispositivo de Aplicación móvil de la consola	Lectura	DeviceIdentity*		
ListDeviceIdentities	Otorga permiso para recuperar una lista de identidades de dispositivos	Enumeración			

Tipos de recursos definidos por Aplicación móvil de AWS Management Console

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
DeviceIdentity	`arn:${Partition}:consoleapp::${Account}:device/${DeviceId}/identity/${IdentityId}`	

Claves de condición para Aplicación móvil de AWS Management Console

La aplicación móvil de la consola no tiene claves de contexto específicas del servicio que se puedan usar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para la facturación consolidada de AWS

AWS La facturación unificada (prefijo de servicio:`consolidatedbilling`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la facturación consolidada de AWS
- Tipos de recursos definidos por la facturación consolidada de AWS
- Claves de condición para la facturación consolidada de AWS

Acciones definidas por la facturación consolidada de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountBillingRole [solo permiso]	Concede permiso para obtener el rol de la cuenta (Payer [Pagador], Linked [Vinculada], Regular [Normal])	Lectura			
ListLinkedAccounts [solo permiso]	Otorga permiso para obtener una lista de cuentas member/linked	Enumeración			

Tipos de recursos definidos por la facturación consolidada de AWS

AWS La facturación unificada no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la facturación consolidada de AWS , especifique `"Resource": "*"` en la política.

Claves de condición para la facturación consolidada de AWS

La facturación consolidada no tiene claves de contexto específicas del servicio que puedan utilizarse en el elemento `Condition` de las instrucciones de políticas. Para ver la lista de claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Control Catalog

AWS El catálogo de control (prefijo de servicio:`controlcatalog`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Control Catalog
- Tipos de recursos definidos por AWS Control Catalog
- Claves de condición para AWS Control Catalog

Acciones definidas por AWS Control Catalog

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetControl	Concede permiso para devolver detalles sobre un control específico	Lectura	control*		
ListCommonControls	Otorga permiso para devolver una lista paginada de los	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	controles más comunes del AWS Catálogo de controles				
ListControlMappings	Otorga permiso para devolver una lista paginada de las asignaciones de controles del Catálogo de controles AWS	Enumeración			
ListControls	Otorga permiso para devolver una lista paginada de todos los controles disponibles en la biblioteca del Catálogo de Control AWS	Enumeración	control*		
ListDomains	Otorga permiso para devolver una lista paginada de dominios del Catálogo de Control AWS	Enumeración			
ListObjectives	Otorga permiso para devolver una lista paginada de objetivos del Catálogo de Control AWS	Enumeración			

Tipos de recursos definidos por AWS Control Catalog

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
common-control	`arn:${Partition}:controlcatalog:::common-control/${CommonControlId}`	
control	`arn:${Partition}:controlcatalog:::control/${ControlId}`	
domain	`arn:${Partition}:controlcatalog:::domain/${DomainId}`	
objective	`arn:${Partition}:controlcatalog:::objective/${ObjectiveId}`	

Claves de condición para AWS Control Catalog

Control Catalog no dispone de claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Control Tower

AWS Control Tower (prefijo de servicio:`controltower`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Control Tower

- Tipos de recursos definidos por AWS Control Tower
- Claves de condición para AWS Control Tower

Acciones definidas por AWS Control Tower

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLandingZone	Concede permiso para crear una zona de aterrizaje	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
CreateManagedAccount [solo permiso]	Otorga permiso para crear una cuenta gestionada por AWS Control Tower	Escritura			
DeleteLandingZone	Concede permiso para eliminar la zona de aterrizaje de AWS Control Tower	Escritura	LandingZone*		
DeregisterManagedAccount [solo permiso]	Otorga permiso para anular el registro de una cuenta creada a través de la fábrica de cuentas de Control Tower AWS	Escritura			
DeregisterOrganizationalUni	Otorga permiso para anular el registro de una unidad organizativa de la administr	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
t [solo permiso]	ación de la Torre de AWS Control				
DescribeAccountFactoryConfig [solo permiso]	Concede permiso para describir la configuración de creación de cuentas actual	Lectura			
DescribeCoreService [solo permiso]	Otorga permiso para describir los recursos gestionados por las cuentas principales de la Torre AWS de Control	Lectura			
DescribeGuardrail [solo permiso]	Concede permiso para describir una barrera de protección	Lectura			
DescribeGuardrailForTarget [solo permiso]	Concede permiso para describir una barrera de protección para una unidad organizativa	Lectura			
DescribeLandingZoneConfiguration [solo permiso]	Concede permiso para describir la configuración de la zona de aterrizaje actual	Lectura			
DescribeManagedAccount [solo permiso]	Concede permiso para describir una cuenta creada a través de la creación de cuentas	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeManagedOrganizationalUnit [solo permiso]	Otorga permiso para describir la unidad AWS organizativa de una organización gestionada por AWS Control Tower	Lectura			
DescribeRegisterOrganizationalUnitOperation [solo permiso]	Concede permiso para describir una operación de una unidad organizativa de registro	Lectura			
DescribeSingleSignOn [solo permiso]	Otorga permiso para describir la configuración actual del Centro de Identidad de IAM de la Torre de AWS Control Tower	Lectura			
DisableBaseline	Concede permiso para desactivar una línea de base en un destino	Escritura	EnabledBaseline*		
DisableControl	Concede permiso para quitar un control de una unidad organizativa	Escritura	EnabledControl*		
DisableGuardrail [solo permiso]	Concede permiso para desactivar una barrera de protección de una unidad organizativa	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableBaseline	Concede permiso para activar una línea de base en un destino	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
EnableControl	Concede permiso para activar un control para una unidad organizativa	Escritura	EnabledControl		controltower:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableGuardrail [solo permiso]	Concede permiso para habilitar una barrera de protección para una unidad organizativa	Escritura			
GetAccountInfo [solo permiso]	Concede permiso para describir el correo electrónico de una cuenta y validar que existe	Lectura			
GetAvailableUpdates [solo permiso]	Otorga permiso para enumerar las actualizaciones disponibles para el despliegue actual AWS de la Torre de Control	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBaseline	Concede permiso para obtener detalles de la línea de base	Lectura	Baseline*		
GetBaselineOperation	Concede permiso para obtener el estado actual de una operación de línea de base concreta	Lectura			
GetControlOperation	Otorga permiso para obtener el estado actual de una DisableControl operación EnabledControl u operación en particular	Lectura			
GetEnabledBaseline	Concede permiso para obtener una línea de base habilitada	Lectura	EnabledBaseline*		
GetEnabledControl	Concede permiso para obtener un control habilitado de una unidad organizativa	Lectura	EnabledControl*		
GetGuardrailComplianceStatus [solo permiso]	Concede permiso para obtener el estado de cumplimiento actual de una barrera de protección	Lectura			
GetHomeRegion [solo permiso]	Otorga permiso para configurar la región de origen de la Torre de AWS Control	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLandingZone	Concede permiso para obtener el estado actual de la configuración de la zona de aterrizaje	Lectura	LandingZone*		
GetLandingZoneDriftStatus	Concede permiso para obtener el estado de desviación de la zona de aterrizaje actual	Lectura			
GetLandingZoneOperation	Concede permiso para obtener el estado actual de una operación específica de zona de aterrizaje	Lectura			
GetLandingZoneStatus [solo permiso]	Concede permiso para obtener el estado actual de la configuración de la zona de aterrizaje	Lectura			
ListBaselines	Concede permiso para enumerar las líneas de base	Enumeración			
ListControlOperations	Concede permiso para enumerar todas las operaciones de control	Enumeración			
ListDirectoryGroups [solo permiso]	Concede permiso para enumerar los grupos de directorio actuales disponibles a través de IAM Identity Center	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDriftDetails	Otorga permiso para enumerar los casos de deriva en la Torre AWS de Control	Lectura			
ListEnabledBaselines	Concede permiso para enumerar líneas de base habilitadas	Enumeración			
ListEnabledControls	Concede permiso para enumerar todos los controles habilitados en una unidad organizativa especificada	Enumeración			
ListEnabledGuardrails [solo permiso]	Concede permiso para enumerar las barreras de protección habilitadas actualmente	Enumeración			
ListExtendGovernancePrecheckDetails [solo permiso]	Concede permiso para enumerar los detalles de comprobación previa de una unidad organizativa	Enumeración			
ListExternalConfigRuleCompliance	Otorga permiso para enumerar el cumplimiento de las reglas de AWS Config externas	Lectura			
ListGuardrailViolations [solo permiso]	Concede permiso para enumerar las infracciones de barreras de protección existentes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGuardrails [solo permiso]	Concede permiso para enumerar todas las barreras de protección disponibles	Enumeración			
ListGuardrailsForTarget [solo permiso]	Concede permiso para enumerar las barreras de protección y su estado actual para una unidad organizativa	Enumeración			
ListLandingZoneOperations	Concede permiso para enumerar todas las operaciones de la zona de aterrizaje	Enumeración			
ListLandingZones	Concede permiso para enumerar todas las zonas de aterrizaje	Enumeración			
ListManagedAccounts [solo permiso]	Otorga permiso para enumerar las cuentas administradas a través de la Torre AWS de Control	Enumeración			
ListManagedAccountsForGuardrail [solo permiso]	Concede permiso para enumerar cuentas administradas con una barrera de protección especificada aplicada	Enumeración			
ListManagedAccountsForParent [solo permiso]	Concede permiso para enumerar cuentas administradas en una unidad organizativa	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListManagedOrganizationalUnits [solo permiso]	Otorga permiso para enumerar las unidades organizativas administradas por la Torre AWS de Control	Enumeración			
ListManagedOrganizationalUnitsForGuardrail [solo permiso]	Concede permiso para enumerar las unidades organizativas administradas con una barrera de protección especificada aplicada	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	EnabledBaseline		
			EnabledControl		
			LandingZone		
ManageOrganizationalUnit [solo permiso]	Concede permiso para configurar una unidad organizativa que será gestionada por AWS Control Tower	Escritura			
PerformPreLaunchChecks [solo permiso]	Concede permiso para realizar validaciones en una cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResetEnabledBaseline	Concede permiso para restablecer una línea de base habilitada	Escritura	EnabledBaseline*		
ResetEnabledControl	Otorga permiso para restablecer un control habilitado para una unidad organizativa	Escritura	EnabledControl*		
ResetLandingZone	Concede permiso para restablecer una zona de aterrizaje	Escritura	LandingZone*		
SetupLandingZone [solo permiso]	Otorga permiso para configurar o actualizar la zona de aterrizaje AWS de la Torre de Control	Escritura			
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:TagKeys	
UpdateAccountFactoryConfig [solo permiso]	Concede permiso para actualizar la configuración de la creación de cuentas	Escritura			
UpdateEnabledBaseline	Concede permiso para actualizar una línea de base habilitada	Escritura	EnabledBaseline*		
UpdateEnabledControl	Concede permiso para actualizar un control habilitado para una unidad organizativa	Escritura	EnabledControl*		
UpdateLandingZone	Concede permiso para actualizar una zona de aterrizaje	Escritura	LandingZone*		

Tipos de recursos definidos por AWS Control Tower

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
EnabledControl	`arn:${Partition}:controltower:${Region}:${Account}:enabledcontrol/${EnabledControlId}`	aws:ResourceTag/${TagKey}
Baseline	`arn:${Partition}:controltower:${Region}::baseline/${BaselineId}`	
EnabledBaseline	`arn:${Partition}:controltower:${Region}:${Account}:enabledbaseline/${EnabledBaselineId}`	aws:ResourceTag/${TagKey}
LandingZone	`arn:${Partition}:controltower:${Region}:${Account}:landingzone/${LandingZoneId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Control Tower

AWS Control Tower define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones para los Informes de costos y usos de AWS

AWS El informe de costos y uso (prefijo de servicio:`cur`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el Informe de costos y usos de AWS
- Tipos de recursos definidos por el Informe de costos y usos de AWS
- Claves de condición para el Informe de costos y usos de AWS

Acciones definidas por el Informe de costos y usos de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReportDefinition	Concede permiso para eliminar la definición del Informe de costos y usos	Escritura	cur*		
DescribeReportDefinitions	Concede permiso para obtener las definiciones del Informe de costos y usos	Lectura			
GetClassicReport [solo permiso]	Concede permiso para obtener un informe CSV de facturación	Lectura			
GetClassicReportPreferences [solo permiso]	Concede permiso para obtener el estado de habilitación del informe clásico para los informes de usos	Lectura			
GetUsageReport [solo permiso]	Otorga permiso para obtener una lista de AWS servicios, tipos de uso y operaciones para el flujo de trabajo del informe de uso. También permite o deniega la descarga de informes de usos	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	cur*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	Concede permiso para modificar la definición del Informe de costos y usos	Escritura	cur*		
PutClassicReportPreferences [solo permiso]	Concede permiso para habilitar los informes clásicos	Escritura			
PutReportDefinition	Concede permiso para escribir la definición del Informe de costos y usos	Escritura	cur*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	cur*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	cur*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey}	
ValidateReportDestination [solo permiso]	Concede permiso para validar si el bucket de S3 tiene los permisos adecuados para generar Informes de costos y usos	Lectura			

Tipos de recursos definidos por el Informe de costos y usos de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

Claves de condición para el Informe de costos y usos de AWS

AWS El informe de costes y uso define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Cost Explorer Service

AWS El servicio Cost Explorer (prefijo de servicio:`ce`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Cost Explorer Service
- Tipos de recursos definidos por AWS Cost Explorer Service
- Claves de condición para AWS Cost Explorer Service

Acciones definidas por AWS Cost Explorer Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAnomalyMonitor	Concede permiso para crear un nuevo monitor de anomalías.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	Concede permiso para crear una nueva suscripción de anomalía.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCostCategoryDefinition	Concede permiso para crear una nueva Cost Category (Categoría de costos) con el nombre y las reglas solicitados.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscript	Concede permiso para crear alertas de caducidad de reserva	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ion [solo permiso]					
CreateReport [solo permiso]	Concede permiso para crear informes de Cost Explorer	Write			
DeleteAnomalyMonitor	Concede permiso para eliminar un monitor de anomalías.	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Concede permiso para eliminar una suscripción de anomalía.	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Concede permiso para eliminar una Cost Category (Categoría de costos).	Write	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [solo permiso]	Concede permiso para eliminar alertas de caducidad de reserva	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReport [solo permiso]	Concede permiso para eliminar informes de Cost Explorer	Write			
DescribeCostCategoryDefinition	Concede permiso para recuperar descripciones como el nombre, el ARN, las reglas, la definición y las fechas en vigor de una Cost Category (Categoría de costos).	Read	costcategory*		
				aws:ResourceTag/${TagKey}	
DescribeNotificationSubscription [solo permiso]	Concede permiso para ver alertas de caducidad de reserva	Read			
DescribeReport [solo permiso]	Concede permiso para ver la página de informes de Cost Explorer	Read			
GetAnomalies	Concede permiso para recuperar anomalías.	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Concede permiso para consultar monitores de anomalía.	Read	anomalymonitor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	Concede permiso para consultar suscripciones a anomalías.	Lectura	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	Otorga permiso para recuperar el recuento aproximado de registros de uso para las preferencias de detalle por recurso, nivel y hora, derivadas del uso del mes anterior	Lectura			
GetCommitmentPurchaseAnalysis	Otorga permiso para recuperar el análisis del compromiso de compra de su cuenta	Lectura			
GetConsoleActionSetEnforced [solo permiso]	Concede permiso para ver si se utilizan acciones de IAM existentes o detalladas para controlar la autorización en las consolas de facturación, administración de costos y cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCostAndUsage	Concede permiso para recuperar las métricas de costo y de uso para su cuenta.	Lectura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageComparisons	Otorga permiso para recuperar las comparaciones de costos y uso de su cuenta	Lectura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageWithResources	Concede permiso para recuperar las métricas de costo y de uso con recursos para su cuenta.	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	Concede permiso para consultar nombres y valores de la Categoría Costos para un periodo especificado.	Lectura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostComparisonDrivers	Otorga permiso para recuperar los factores de coste de su cuenta	Lectura	billingview		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCostForecast	Concede permiso para recuperar una previsión de costo para un periodo de tiempo de previsión.	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetDimensionValues	Concede permiso para recuperar todos los valores de filtro disponibles de un filtro de un periodo.	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetPreferences [solo permiso]	Concede permiso para ver la página de preferencias de Cost Explorer	Read			
GetReservationCoverage	Concede permiso para recuperar la cobertura de reserva para su cuenta.	Read			
GetReservationPurchaseRecommendation	Concede permiso para recuperar las recomendaciones de reserva para su cuenta.	Read			
GetReservationUtilization	Concede permiso para recuperar la utilización de reserva para su cuenta.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRightsizingRecommendation	Concede permiso para recuperar las recomendaciones de adecuación de tamaño para su cuenta.	Lectura			
GetSavingsPlanPurchaseRecommendationDetails	Otorga permiso para recuperar los detalles de la recomendación de Savings Plans para su cuenta	Lectura			
GetSavingsPlansCoverage	Concede permiso para recuperar la cobertura de Savings Plans para su cuenta.	Read			
GetSavingsPlansPurchaseRecommendation	Concede permiso para recuperar las recomendaciones de Savings Plans para su cuenta.	Read			
GetSavingsPlansUtilization	Concede permiso para recuperar la utilización de Savings Plans para su cuenta.	Read			
GetSavingsPlansUtilizationDetails	Concede permiso para recuperar los detalles de utilización de Savings Plans de su cuenta.	Read			
GetTags	Concede permiso para consultar las etiquetas de un periodo de tiempo especificado.	Read	billingview		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetUsageForecast	Concede permiso para recuperar una previsión de uso para un periodo de tiempo de previsión.	Lectura	billingview		
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	Otorga permiso para recuperar una lista de sus análisis históricos de compromisos de compra	Enumeración			
ListCostAllocationTagBackfillHistory	Concede permiso para enumerar el historial de relleno de la etiqueta de asignación de costos	Enumeración			
ListCostAllocationTags	Concede permiso para enumerar las etiquetas para la asignación de costos	Enumeración			
ListCostCategoryDefinitions	Concede permiso para recuperar nombres, ARN y fechas en vigor para todas las Cost Categories (Categorías de costos).	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSavingsPlansPurchaseRecommendationGeneration	Otorga permiso para enumerar las generaciones de sus recomendaciones históricas	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso de Cost Explorer	Lectura	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	Concede permiso para proporcionar comentarios sobre anomalías detectadas.	Escritura			
StartCommitmentPurchaseAnalysis	Otorga permiso para solicitar un análisis de compromiso de compra	Escritura			
StartCostAllocationTagBackfill	Concede permiso para solicitar un relleno de la etiqueta de asignación de costos	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartSavingsPlansPurchaseRecommendationGeneration	Otorga permiso para solicitar una generación de recomendaciones sobre Savings Plans	Escritura			
TagResource	Concede permiso para etiquetar un recurso de Cost Explorer	Etiquetado	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso de Cost Explorer	Etiquetado	anomalymonitor		
			anomalysubscription		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	Concede permiso para actualizar un monitor de anomalías existente.	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	Concede permiso para actualizar una suscripción de anomalía existente.	Escritura	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [solo permiso]	Concede permiso para cambiar si se utilizarán acciones de IAM existentes o detalladas para controlar la autorización en las consolas de facturación, administración de costos y cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCostAllocationTagsStatus	Concede permiso para actualizar el estado de etiquetas de asignación de costos existentes	Escritura			
UpdateCostCategoryDefinition	Concede permiso para actualizar una Cost Category existente (Categoría de costos).	Write	costcategory*		
				aws:ResourceTag/${TagKey}	
UpdateNotificationSubscription [solo permiso]	Concede permiso para actualizar alertas de caducidad de reserva	Write			
UpdatePreferences [solo permiso]	Concede permiso para editar la página de preferencias de Cost Explorer	Write			
UpdateReport [solo permiso]	Concede permiso para actualizar informes de Cost Explorer	Write			

Tipos de recursos definidos por AWS Cost Explorer Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
anomalysubscription	`arn:${Partition}:ce::${Account}:anomalysubscription/${Identifier}`	aws:ResourceTag/${TagKey}
anomalymonitor	`arn:${Partition}:ce::${Account}:anomalymonitor/${Identifier}`	aws:ResourceTag/${TagKey}
costcategory	`arn:${Partition}:ce::${Account}:costcategory/${Identifier}`	aws:ResourceTag/${TagKey}
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Cost Explorer Service

AWS El servicio Cost Explorer define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el Centro de optimización de costos de AWS

AWS Cost Optimization Hub (prefijo de servicio:`cost-optimization-hub`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el Centro de optimización de costos de AWS
- Tipos de recursos definidos por Centro de optimización de costos de AWS
- Claves de condición del centro de optimización de costos de AWS

Acciones definidas por el Centro de optimización de costos de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPreferences	Otorga permiso para obtener preferencias	Lectura			
GetRecommendation	Otorga permiso para obtener la configuración de los recursos y el impacto estimado en los costos para una recomendación	Lectura			
ListEnrollmentStatuses	Otorga permiso para enumerar los estados de inscripción de la cuenta especificada o de todos los miembros de una cuenta de administración	Enumeración			
ListRecommendationSummaries	Otorga permiso para enumerar resúmenes de recomendación por grupo	Enumeración			cost-optimization-hub:GetRecommendation
ListRecommendations	Concede permiso para enumerar una vista de resumen de recomendaciones	Enumeración			cost-optimization-hub:GetRecommendation
UpdateEnrollmentStatus	Concede permiso para actualizar el estado de inscripción.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePreferences	Concede permiso para actualizar preferencias	Escritura			

Tipos de recursos definidos por Centro de optimización de costos de AWS

AWS Cost Optimization Hub no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al centro de optimización de costos de AWS , especifique `"Resource": "*"` en la política.

Claves de condición del centro de optimización de costos de AWS

El centro de optimización de costos no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el Servicio de verificación de clientes de AWS

AWS El Servicio de verificación de clientes (prefijo de servicio:`customer-verification`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el Servicio de verificación de clientes de AWS
- Tipos de recurso definidos por el Servicio de verificación de clientes de AWS
- Claves de condición para el Servicio de verificación de clientes de AWS

Acciones definidas por el Servicio de verificación de clientes de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCustomerVerificationDetails [solo permiso]	Concede permiso para crear datos de verificación de clientes	Escritura			
CreateUploadUrls [solo permiso]	Otorga permiso para crear una carga URLs	Escritura			
GetCustomerVerificationDetails [solo permiso]	Concede permiso para obtener datos de verificación de clientes	Lectura			
GetCustomerVerificationEligibility [solo permiso]	Concede permiso para obtener la elegibilidad de verificación de clientes	Lectura			
UpdateCustomerVerificationD	Concede permiso para actualizar datos de verificación de clientes	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
etails [solo permiso]					

Tipos de recurso definidos por el Servicio de verificación de clientes de AWS

AWS El Servicio de verificación de clientes no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al Servicio de verificación de clientes de AWS , especifique `"Resource": "*"` en la política.

Claves de condición para el Servicio de verificación de clientes de AWS

El Servicio de verificación de clientes no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Data Exchange

AWS Data Exchange (prefijo de servicio:`dataexchange`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Data Exchange
- Tipos de recursos definidos por AWS Data Exchange

- Claves de condición para AWS Data Exchange

Acciones definidas por AWS Data Exchange

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptDataGrant	Concede permiso para aceptar una concesión de datos	Escritura	data-grants*		
CancelJob	Concede permiso para cancelar un trabajo	Escritura	jobs*		
CreateAsset [solo permiso]	Concede permiso para crear un activo (por ejemplo, en un trabajo)	Escritura	revisions*		
CreateDataGrant	Concede permiso para crear una concesión de datos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	dataexchange:PublishToDataGrant
CreateDataSet	Concede permiso para crear un conjunto de datos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventAction	Concede permiso para crear una acción de evento	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateJob	Concede permiso para crear un trabajo para importar o exportar activos.	Escritura		dataexchange:JobType	
CreateRevision	Concede permiso para crear una revisión	Escritura	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Concede permiso para eliminar un activo	Escritura	assets*		
DeleteDataGrant	Concede permiso para eliminar una concesión de datos	Escritura	data-grants*		
DeleteDataSet	Concede permiso para eliminar un conjunto de datos.	Escritura	data-sets*		
			entitled-data-sets*		
DeleteEventAction	Concede permiso para eliminar una acción de evento	Escritura	event-actions*		
DeleteRevision	Concede permiso para eliminar una revisión.	Escritura	revisions*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAsset	Concede permiso para obtener información sobre un activo y exportarlo (p. ej., en un trabajo).	Lectura	assets*		
			entitled-assets*		
GetDataGrant	Concede permiso para obtener una concesión de datos	Lectura	data-grants*		
GetDataSet	Concede permiso para obtener información sobre un conjunto de datos	Lectura	data-sets*		
			entitled-data-sets*		
GetEventAction	Concede permiso para obtener una acción de evento	Lectura	event-actions*		
GetJob	Concede permiso para obtener información sobre un trabajo.	Lectura	jobs*		
GetReceivedDataGrant	Concede permiso para obtener una concesión de datos recibidos	Lectura	data-grants*		
GetRevision	Concede permiso para obtener información sobre una revisión	Lectura	entitled-revisions*		
			revisions*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDataGrants	Concede permiso para enumerar las concesiones de datos de la cuenta	Enumeración			
ListDataSetRevisions	Concede permiso para enumerar las revisiones de un conjunto de datos.	Enumeración	data-sets *		
			entitled-data-sets *		
ListDataSets	Concede permiso para enumerar conjuntos de datos de la cuenta	Enumeración			
ListEventActions	Concede permiso para enumerar las acciones de evento de la cuenta	Enumeración			
ListJobs	Concede permiso para enumerar los trabajos de la cuenta.	Enumeración			
ListReceivedDataGrants	Concede permiso para enumerar las concesiones de datos recibidas para la cuenta	Enumeración			
ListRevisionAssets	Concede permiso para obtener una lista de los activos de una revisión.	Enumeración	entitled-revisions *		
			revisions *		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para obtener una lista de las etiquetas que ha asociado con el recurso especificado	Enumeración	data-grants		
			data-sets		
			revisions		
PublishDataSet [solo permiso]	Concede permiso para publicar un conjunto de datos en un producto	Escritura	data-sets*		
PublishToDataGrant [solo permiso]	Concede permiso para publicar un conjunto de datos en una concesión de datos	Escritura	data-sets*		
RevokeRevision	Concede permiso para revocar el acceso de los suscriptores a una revisión	Escritura	revisions*		
SendApiAsset	Concede permiso para enviar una solicitud a un activo de API.	Escritura	assets*		
			entitled-assets*		
SendDataSetNotification	Concede permiso para enviar una notificación a los suscriptores de un conjunto de datos.	Escritura	data-sets*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartJob	Concede permiso para comenzar un trabajo.	Escritura	jobs*		dataexchange:CreateAsset dataexchange:DeleteDataSet dataexchange:GetAsset dataexchange:GetDataSet dataexchange:GetRevision dataexchange:PublishDataSet redshift:AuthorizeDataShare
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso especificado	Etiquetado	data-grants		
			data-sets		
			revisions		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una o más etiquetas de un recurso especificado.	Etiquetado	data-grants		
			data-sets		
			revisions		
				aws:TagKeys	
UpdateAsset	Concede permiso para obtener información actualizada sobre un activo.	Escritura	assets*		
UpdateDataSet	Concede permiso para actualizar la información sobre un conjunto de datos.	Escritura	data-sets*		
UpdateEventAction	Concede permiso para actualizar la información para una acción de evento	Escritura	event-actions*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRevision	Concede permiso para actualizar la información sobre una revisión.	Escritura	revisions *		dataexchange:PublishDataSet dataexchange:PublishToDataGrant

Tipos de recursos definidos por AWS Data Exchange

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
jobs	`arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}`	dataexchange:JobType
data-sets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}`	aws:ResourceTag/${TagKey}
entitled-data-sets	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}`	

Tipos de recurso	ARN	Claves de condición
revisions	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}	aws:ResourceTag/${TagKey}
entitled-revisions	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}	
assets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
entitled-assets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
event-actions	arn:${Partition}:dataexchange:${Region}:${Account}:event-actions/${EventActionId}	
data-grants	arn:${Partition}:dataexchange:${Region}:${Account}:data-grants/${DataGrantId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Data Exchange

AWS Data Exchange define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso de creación de solicitudes en función del conjunto de valores permitidos para cada una de las etiquetas obligatorias	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra el acceso según la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
dataexchange:JobType	Filtra el acceso según el tipo de trabajo especificado	Cadena

Claves de condición, recursos y acciones de Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager (prefijo de servicio: `dlm`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Data Lifecycle Manager
- Tipos de recursos definidos por Amazon Data Lifecycle Manager
- Claves de condición de Amazon Data Lifecycle Manager

Acciones definidas por Amazon Data Lifecycle Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLifecyclePolicy	Otorga permiso para crear una política de ciclo de vida de datos para administrar la creación programada y la retención de instantáneas de Amazon EBS. Puede tener hasta 100 políticas	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	Concede permiso para eliminar una política de ciclo de vida de datos existente. Además, esta acción detiene la creación y la eliminación de las instantáneas que la política especificaba. Las instantáneas existentes no se ven afectadas	Escritura	policy*		
GetLifecyclePolicies	Concede permiso para una lista de descripciones resumidas de las políticas de ciclo de vida de datos	Enumeración			
GetLifecyclePolicy	Concede permiso para un retorno de una descripción completa de una única política de ciclo de vida de datos.	Lectura	policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para enumerar las etiquetas asociadas a un recurso.	Lectura	policy*		
TagResource	Otorga permiso para agregar o actualizar las etiquetas de un recurso.	Etiquetado	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas asociadas a un recurso	Etiquetado	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	Otorga permisos para actualizar una política de ciclo de vida de datos existentes	Escritura	policy*		

Tipos de recursos definidos por Amazon Data Lifecycle Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Data Pipeline

AWS Data Pipeline (prefijo de servicio:`datapipeline`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Data Pipeline
- Tipos de recursos definidos por AWS Data Pipeline
- Claves de condición para AWS Data Pipeline

Acciones definidas por AWS Data Pipeline

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivatePipeline	Otorga permiso para validar la canalización especificada y comienza a procesar las tareas de canalización. Si la canalización no supera la validación, la activación da error	Escritura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTags	Otorga permiso para agregar o modificar etiquetas para la canalización especificada	Etiquetado	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
CreatePipeline	Otorga permiso para crear una nueva canalización de imagen	Escritura		aws:RequestTag/${TagKey} aws:TagKeys datapipeline:Tag/${TagKey}	datapipeline:AddTags
DeactivatePipeline	Otorga permiso para desactivar la canalización en ejecución especificada	Escritura	pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
DeletePipeline	Otorga permiso para eliminar una canalización, su definición de canalización y su historial de ejecuciones	Escritura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribeObjects	Otorga permiso para obtener las definiciones de objeto para un conjunto de objetos asociados a la canalización	Lectura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePipelines	Otorga permiso para recuperar los metadatos de una o varias canalizaciones	Lectura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
EvaluateExpression	Otorga permiso a los ejecutores de tareas para llamar EvaluateExpression y evaluar una cadena en el contexto del objeto especificado	Lectura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
GetAccountLimits [solo permiso]	Otorga permiso para llamar GetAccountLimits	Enumeración			
GetPipelineDefinition	Otorga permiso para obtener la definición de la canalización especificada	Lectura	pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
ListPipelines	Otorga permiso para enumerar los identificadores de canalización de todas las canalizaciones activos para los que tiene permiso de acceso	Enumeración			
PollForTask	Otorga permiso a los ejecutores de tareas para llamar PollForTask y recibir una tarea que realizar de AWS Data Pipeline	Escritura		datapipeline:workerGroup	
PutAccountLimits [solo permiso]	Otorga permiso para llamar PutAccountLimits	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutPipelineDefinition	Otorga permiso para agregar tareas, programas y condiciones previas a la canalización especificada	Escritura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
QueryObjects	Otorga permiso para consultar en la canalización especificada los nombres de los objetos que coinciden con el conjunto específico de condiciones	Lectura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
RemoveTags	Otorga permisos para quitar etiquetas de la canalización especificada	Etiquetado	pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
ReportTaskProgress	Concede permiso a los ejecutores de tareas para que ReportTaskProgress llamen cuando se les asigna una tarea para confirmar que la tienen	Escritura	pipeline*		
ReportTaskRunnerHeartbeat	Concede permiso a los encargados de ejecutar las tareas para que llamen ReportTaskRunnerHeartbeat cada 15 minutos para indicar que están en funcionamiento	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetStatus	Otorga permiso para solicitar que el estado de los objetos de canalización físicos o lógicos especificados deben actualizarse en la canalización especificada	Escritura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
SetTaskStatus	Otorga permiso a los ejecutores de tareas SetTaskStatus para llamar para notificar a AWS Data Pipeline que una tarea se ha completado y proporcionar información sobre el estado final	Escritura	pipeline*		
ValidatePipelineDefinition	Otorga permiso para validar la definición de la canalización especificada para asegurarse de que está bien formada y se puede ejecutar sin errores	Lectura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Tipos de recursos definidos por AWS Data Pipeline

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
pipeline	`arn:${Partition}:datapipeline:${Region}:${Account}:pipeline/${PipelineId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Data Pipeline

AWS Data Pipeline define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
datapipeline:PipelineCreator	Filtra el acceso por usuario de IAM que ha creado la canalización	ArrayOfString
datapipeline:Tag/${TagKey}	Filtra el acceso por el key/value par especificado por el cliente que se puede adjuntar a un recurso	Cadena
datapipeline:workerGroup	Filtra el acceso por nombre de un grupo de empleados para los que el ejecutor de tareas recupera trabajo	ArrayOfString

Acciones, recursos y claves de condición para AWS Database Migration Service

AWS Database Migration Service (prefijo de servicio:`dms`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Database Migration Service
- Tipos de recursos definidos por AWS Database Migration Service
- Claves de condición para AWS Database Migration Service

Acciones definidas por AWS Database Migration Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTagsToResource	Otorga permiso para agregar etiquetas de metadatos a recursos de DMS, incluidas instancias de replicación, puntos de enlace, grupos de seguridad y tareas de migración.	Etiquetado	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApplyPendingMaintenanceAction	Otorga permiso para aplicar una acción de mantenimiento pendiente a un recurso (por ejemplo, a una instancia de replicación).	Escritura	ReplicationInstance*		
AssociateExtensionPack	Otorga permiso para asociar un paquete de extensión	Escritura	MigrationProject*		
BatchStartRecommendations	Concede permiso para iniciar el análisis de hasta 20 bases de datos de origen a fin de recomendar motores de destino para cada base de datos de origen	Escritura			
CancelReplicationTaskAssessmentRun	Otorga permiso para cancelar una única ejecución de evaluación previa a la migración.	Escritura	ReplicationTaskAssessmentRun*		
CreateDataMigration	Concede permiso para crear una migración de base de datos mediante la configuración proporcionada	Escritura	MigrationProject*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateDataProvider	Otorga permiso para crear un proveedor de datos mediante la configuración proporcionada	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEndpoint	Otorga permiso para crear un punto de enlace utilizando la configuración proporcionada.	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateEventSubscription	Otorga permiso para crear una suscripción a la notificación de eventos del AWS DMS	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFleetAdvisorCollector	Concede permiso para crear un recopilador de Fleet Advisor utilizando los parámetros especificados	Escritura			iam:PassRole
CreateInstanceProfile	Otorga permiso para crear un perfil de instancia mediante la configuración proporcionada	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateMigrationProject	Otorga permiso para crear un proyecto de migración mediante la configuración proporcionada	Escritura	DataProvider* InstanceProfile*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationConfig	Concede permiso para crear una configuración de replicación mediante la configuración proporcionada	Escritura	Endpoint*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateReplicationInstance	Otorga permiso para crear una instancia de replicación utilizando los parámetros especificados.	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateReplicationSubnetGroup	Concede permiso para crear un grupo de subredes de replicación con una lista de la subred de una IDs VPC	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationTask		Write	Endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para crear una tarea de replicación utilizando los parámetros especificados.		ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	Concede permiso para eliminar el certificado especificado.	Write	Certificate*		
DeleteConnection	Otorga permiso para eliminar la conexión especificada entre una instancia de reproducción y un punto de enlace.	Escritura	Endpoint*		
			ReplicationInstance*		
DeleteDataMigration	Concede permiso para eliminar la migración de base de datos especificada	Escritura	DataMigration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDataProvider	Otorga permiso para eliminar el proveedor de datos especificado	Escritura	DataProvider*		
DeleteEndpoint	Otorga permiso para eliminar el punto de enlace especificado.	Escritura	Endpoint*		
DeleteEventSubscription	Otorga permiso para eliminar una suscripción a un AWS evento de DMS	Escritura	EventSubscription*		
DeleteFleetAdvisorCollector	Concede permiso para eliminar el recopilador de Fleet Advisor especificado	Escritura			
DeleteFleetAdvisorDatabases	Concede permiso para eliminar las bases de datos de Fleet Advisor especificadas	Escritura			
DeleteInstanceProfile	Concede permiso para eliminar el perfil de instancia especificado.	Escritura	InstanceProfile*		
DeleteMigrationProject	Otorga permiso para eliminar el proyecto de migración especificado	Escritura	MigrationProject*		
DeleteReplicationConfig	Concede permiso para eliminar la configuración de replicación especificada	Escritura	ReplicationConfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReplicationInstance	Otorga permiso para eliminar la instancia de replicación especificada.	Write	ReplicationInstance*		
DeleteReplicationSubnetGroup	Otorga permiso para eliminar un grupo de subredes.	Write	ReplicationSubnetGroup*		
DeleteReplicationTask	Otorga permiso para eliminar la tarea de replicación especificada.	Write	ReplicationTask*		
DeleteReplicationTaskAssessmentRun	Otorga permiso para eliminar el registro de una única ejecución de evaluación previa a la migración.	Escritura	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	Otorga permiso para enumerar todos los atributos del AWS DMS de una cuenta de cliente	Lectura			
DescribeApplicableIndividualAssessments	Otorga permiso para mostrar una lista de evaluaciones individuales que puede especificar para una nueva ejecución de evaluación previa a la migración.	Read	ReplicationInstance		
			ReplicationTask		
DescribeCertificates	Otorga permiso para proporcionar una descripción del certificado.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConnections	Otorga permiso para describir el estado de las conexiones que se han realizado entre la instancia de replicación y un punto de enlace.	Lectura			
DescribeConversionConfiguration	Concede permiso para devolver información sobre la configuración del proyecto de conversión de esquemas de DMS	Lectura	MigrationProject*		
DescribeDataMigrations	Concede permiso para devolver información sobre las migraciones de base de datos correspondientes a su cuenta en la región especificada	Lectura			
DescribeEndpointSettings	Otorga permiso para devolver la posible configuración de punto de enlace disponible al crear un punto de enlace para un motor de base de datos específico	Lectura			
DescribeEndpointTypes	Otorga permiso para devolver información sobre el tipo de puntos de enlace disponibles.	Read			
DescribeEndpoints	Otorga permiso para devolver información sobre los puntos de enlace de su cuenta en la región actual.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEngineVersions	Concede permiso para devolver información sobre las versiones disponibles para las instancias de replicación de DMS	Lectura			
DescribeEventCategories	Otorga permiso para mostrar una lista de categorías de todos los tipos de origen de eventos o, si se especifica, para tipo de origen especificado.	Read			
DescribeEventSubscriptions	Otorga permiso para mostrar una lista de todas las descripciones de suscripción de una cuenta de cliente.	Read			
DescribeEvents	Otorga permiso para mostrar una lista de eventos para un identificador de origen y tipo de origen determinados.	Lectura			
DescribeFleetAdvisorCollectors	Concede permiso para devolver una lista paginada de recopiladores de Fleet Advisor de la cuenta de acuerdo con la configuración del filtro	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFleetAdvisorDatabases	Concede permiso para devolver una lista paginada de bases de datos de Fleet Advisor de la cuenta de acuerdo con la configuración del filtro	Lectura			
DescribeFleetAdvisorLsaAnalysis	Concede permiso para devolver una lista paginada de descripciones de análisis de evaluación a gran escala (LSA) producidos por los recopiladores de Fleet Advisor	Lectura			
DescribeFleetAdvisorSchemaObjectSummary	Concede permiso para devolver una lista paginada de descripciones de esquemas descubiertos por los recopiladores de Fleet Advisor de acuerdo con la configuración del filtro	Lectura			
DescribeFleetAdvisorSchemas	Concede permiso para devolver una lista paginada de esquemas descubiertos por los recopiladores de Fleet Advisor de acuerdo con la configuración del filtro	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMetadataModelImports	Concede permiso para devolver información sobre el inicio de las operaciones de importación del modelo de metadatos para un proyecto de migración	Lectura	Migration Project*		
DescribeOrderableReplicationInstances	Otorga permiso para devolver información sobre los tipos de instancias de replicación que se pueden crear en la región especificada.	Lectura			
DescribePendingMaintenanceActions	Otorga permiso para devolver información sobre acciones de mantenimiento pendientes	Lectura			
DescribeRecommendationLimitations	Otorga permiso para devolver una lista paginada con descripciones de las limitaciones para recomendaciones de los motores de destino AWS	Lectura			
DescribeRecommendations	Concede permiso para devolver una lista paginada de descripciones de recomendaciones de motores de destino para las bases de datos de origen	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRefreshSchemasStatus	Otorga permiso para devolver el estado de la operación RefreshSchemas	Lectura	Endpoint*		
DescribeReplicationConfigs	Concede permiso para describir las configuraciones de replicación	Lectura			
DescribeReplicationInstanceTaskLogs	Otorga permiso para devolver información sobre los registros de tareas de la tarea especificada.	Read	ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	Otorga permiso para devolver información sobre las instancias de replicación para su cuenta en la región actual.	Read			
DescribeReplicationSubnetGroups	Otorga permiso para devolver información sobre los grupos de subred de replicación.	Lectura			
DescribeReplicationTableStatistics	Concede permiso para describir las estadísticas de las tablas de replicación	Lectura	ReplicationConfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReplicationTaskAssessmentResults	Otorga permiso para devolver los últimos resultados de evaluación de tareas de Amazon S3.	Read	ReplicationTask		
DescribeReplicationTaskAssessmentRuns	Otorga permiso para devolver una lista paginada de ejecuciones de evaluación previa a la migración en función de la configuración del filtro.	Read	ReplicationInstance		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTaskIndividualAssessments	Otorga permiso para devolver una lista paginada de evaluaciones individuales en función de la configuración del filtro.	Read	ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTasks	Otorga permiso para devolver información sobre tareas de replicación de su cuenta en la región actual.	Lectura			
DescribeReplications	Concede permiso para describir las replicaciones	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSchemas	Otorga permiso para devolver información sobre el esquema del punto de enlace especificado.	Read	Endpoint*		
DescribeTableStatistics	Otorga permiso para devolver las estadísticas de la tabla en la tarea de migración de la base de datos, incluido el nombre de la tabla, las filas insertadas, las filas actualizadas y las filas eliminadas.	Lectura	ReplicationTask*		
ExportMetadataModelAssessment	Otorga permiso para exportar la evaluación del modelo de metadatos especificado	Escritura	MigrationProject		
ImportCertificate	Otorga permiso para cargar el certificado especificado.	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	Otorga permiso para enumerar los atributos del AWS DMS de un proveedor de datos	Lectura	DataProvider		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExtensionPacks	Otorga permiso para enumerar los atributos AWS de DMS de un paquete de extensiones	Lectura	MigrationProject		
ListInstanceProfiles	Otorga permiso para enumerar los atributos de AWS DMS para los perfiles de una instancia	Lectura	InstanceProfile		
ListMetadataModelAssessmentActionItems [solo permiso]	Otorga permiso para enumerar los atributos del AWS DMS para los elementos de acción de evaluación de un modelo de metadatos. Nota. A pesar de que esta acción es obligatoria StartMetadataModelImport, esta última no autoriza actualmente la operación de conversión de esquemas descrita	Lectura	MigrationProject		dms:StartMetadataModelImport
ListMetadataModelAssessments	Otorga permiso para enumerar los atributos del AWS DMS para las evaluaciones de un modelo de metadatos	Lectura	MigrationProject		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMetadataModelConversions	Otorga permiso para enumerar los atributos del AWS DMS para las conversiones de un modelo de metadatos	Lectura	MigrationProject		
ListMetadataModelExports	Otorga permiso para enumerar los atributos del AWS DMS para las exportaciones de un modelo de metadatos	Lectura	MigrationProject		
ListMigrationProjects	Otorga permiso para enumerar los atributos del AWS DMS para un proyecto de migración. Nota. A pesar de ello, esta acción requiere DescribeMigrationProjects y DescribeConversionConfiguration, ambas acciones obligatorias, actualmente no autorizan la operación de conversión de esquemas descrita	Lectura	DataProvider		dms:DescribeConversionConfiguration
			InstanceProfile		
			MigrationProject		
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas de un recurso AWS de DMS	Lectura	Certificate		
			DataMigration		
			DataProvider		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyDataMigration	Concede permiso para modificar la migración de base de datos especificada	Escritura	DataMigration*		iam:PassRole
ModifyEndpoint	Otorga permiso para modificar el punto de enlace especificado.	Escritura	Endpoint*		iam:PassRole
			Certificate		
ModifyEventSubscription	Otorga permiso para modificar una suscripción de notificación de eventos AWS de DMS existente	Escritura			
ModifyFleetAdvisorCollector [solo permiso]	Concede permiso para modificar el nombre y la descripción del recopilador de Fleet Advisor especificado	Escritura			
ModifyFleetAdvisorCollectorStatuses [solo permiso]	Concede permiso para modificar el estado del recopilador de Fleet Advisor especificado	Escritura			
ModifyReplicationConfig	Concede permiso para modificar la configuración de replicación especificada	Escritura	ReplicationConfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyReplicationInstance	Otorga permiso para modificar la instancia de replicación para aplicar una nueva configuración.	Write	ReplicationInstance*		
ModifyReplicationSubnetGroup	Otorga permiso para modificar la configuración del grupo de subred de replicación especificado.	Write			
ModifyReplicationTask	Otorga permiso para modificar la tarea de replicación especificada.	Write	ReplicationTask*		
MoveReplicationTask	Otorga permiso para mover la tarea de reproducción especificada a una instancia de reproducción diferente.	Write	ReplicationInstance*		
			ReplicationTask*		
RebootReplicationInstance	Otorga permiso para reiniciar una instancia de replicación. El reinicio produce una interrupción momentánea, hasta que la instancia de replicación vuelva a estar disponible.	Write	ReplicationInstance*		
RefreshSchemas	Otorga permiso para rellenar el esquema del punto de enlace especificado.	Escritura	Endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ReplicationInstance*		
ReloadReplicationTables	Concede permiso para volver a cargar la tabla de base de datos de destino con el origen para una replicación	Escritura	ReplicationConfig*		
ReloadTables	Otorga permiso para volver a cargar la tabla de base de datos de destino con los datos de origen.	Write	ReplicationTask*		
RemoveTagsFromResource	Otorga permiso para eliminar etiquetas de metadatos de un recurso de DMS.	Etiquetado	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RunFleetAdvisorLsaAnalysis	Concede permiso para realizar un análisis de evaluación a gran escala (LSA) de todos los recopiladores de Fleet Advisor de la cuenta	Escritura			
StartDataMigration	Concede permiso para iniciar la migración de base de datos	Escritura	DataMigration*		
StartMetadataModelAssessment	Otorga permiso para iniciar una nueva evaluación del modelo de metadatos	Escritura	MigrationProject*		
StartMetadataModelConversion	Otorga permiso para iniciar una nueva conversión del modelo de metadatos	Escritura	MigrationProject*		
StartMetadataModelExportAsScripts	Otorga permiso para iniciar una nueva exportación del modelo de metadatos como script	Escritura	MigrationProject*		
StartMetadataModelExportToTarget	Otorga permiso para iniciar una nueva exportación del modelo de metadatos al destino	Escritura	MigrationProject*		
StartMetadataModelImport	Otorga permiso para iniciar una nueva importación del modelo de metadatos	Escritura	MigrationProject*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartRecommendations	Concede permiso para iniciar el análisis de la base de datos de origen a fin de proporcionar recomendaciones de motores de destino	Escritura			
StartReplication	Concede permiso para iniciar una replicación	Escritura	ReplicationConfig*		
StartReplicationTask	Otorga permiso para comenzar la tarea de replicación.	Write	ReplicationTask*		
StartReplicationTaskAssessment	Otorga permiso para comenzar la evaluación de la tarea de replicación de los tipos de datos no admitidos en la base de datos de origen.	Write	ReplicationTask*		
StartReplicationTaskAssessmentRun	Otorga permiso para comenzar una nueva ejecución de evaluación previa a la migración para una o más evaluaciones individuales de una tarea de migración.	Escritura	ReplicationTask*		iam:PassRole
StopDataMigration	Concede permiso para detener la migración de base de datos	Escritura	DataMigration*		
StopReplication	Concede permiso para detener una replicación	Escritura	ReplicationConfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopReplicationTask	Otorga permiso para detener la tarea de replicación.	Write	ReplicationTask*		
TestConnection	Otorga permiso para probar la conexión entre la instancia de replicación y el punto de enlace.	Lectura	Endpoint*		
			ReplicationInstance*		
UpdateConversionConfiguration	Otorga permiso para actualizar una configuración de conversión	Escritura	MigrationProject*		
UpdateDataProvider	Otorga permiso para actualizar el proveedor de datos especificado	Escritura	DataProvider*		
UpdateInstanceProfile	Otorga permiso para actualizar el perfil de instancia especificado	Escritura	InstanceProfile*		
UpdateMigrationProject	Otorga permiso para actualizar el proyecto de migración especificado	Escritura	MigrationProject*		
UpdateSubscriptionsToEventBridge	Concede permiso para migrar las suscripciones de DMS a Eventbridge	Escritura			
UploadFileMetadataList [solo permiso]	Concede permiso para cargar archivos al bucket de Amazon S3	Escritura			

Tipos de recursos definidos por AWS Database Migration Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Certificate	`arn:${Partition}:dms:${Region}:${Account}:cert:*`	aws:ResourceTag/${TagKey} dms:cert-tag/${TagKey}
DataProvider	`arn:${Partition}:dms:${Region}:${Account}:data-provider:*`	aws:ResourceTag/${TagKey} dms:data-provider-tag/${TagKey}
DataMigration	`arn:${Partition}:dms:${Region}:${Account}:data-migration:*`	aws:ResourceTag/${TagKey} dms:data-migration-tag/${TagKey}
Endpoint	`arn:${Partition}:dms:${Region}:${Account}:endpoint:*`	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	`arn:${Partition}:dms:${Region}:${Account}:es:*`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
		dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}
MigrationProject	arn:${Partition}:dms:${Region}:${Account}:migration-project:*	aws:ResourceTag/${TagKey} dms:migration-project-tag/${TagKey}
ReplicationConfig	arn:${Partition}:dms:${Region}:${Account}:replication-config:*	aws:ResourceTag/${TagKey} dms:replication-config-tag/${TagKey}
ReplicationInstance	arn:${Partition}:dms:${Region}:${Account}:rep:*	aws:ResourceTag/${TagKey} dms:rep-tag/${TagKey}
ReplicationSubnetGroup	arn:${Partition}:dms:${Region}:${Account}:subgrp:*	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	arn:${Partition}:dms:${Region}:${Account}:task:*	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}

Tipos de recurso	ARN	Claves de condición
ReplicationTaskAssessmentRun	`arn:${Partition}:dms:${Region}:${Account}:assessment-run:*`	aws:ResourceTag/${TagKey} dms:assessment-run-tag/${TagKey}
ReplicationTaskIndividualAssessment	`arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*`	aws:ResourceTag/${TagKey} dms:individual-assessment-tag/${TagKey}

Claves de condición para AWS Database Migration Service

AWS Database Migration Service define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la presencia de los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
dms:assessment-run-tag/${TagKey}	Filtra el acceso según la presencia de pares clave-valor de etiqueta en la solicitud de AssessmentRun	Cadena
dms:cert-tag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud para Certificate	Cadena
dms:data-migration-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de DataMigration	Cadena
dms:data-provider-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de DataProvider	Cadena
dms:endpoint-tag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud para Endpoint	Cadena
dms:es-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de EventSubscription	Cadena
dms:individual-assessment-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de IndividualAssessment	Cadena
dms:instance-profile-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de InstanceProfile	Cadena
dms:migration-project-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de MigrationProject	Cadena
dms:rep-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de ReplicationInstance	Cadena

Claves de condición	Descripción	Tipo
dms:replication-config-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de ReplicationConfig	Cadena
dms:req-tag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud determinada	Cadena
dms:subgrp-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de ReplicationSubnetGroup	Cadena
dms:task-tag/${TagKey}	Filtra el acceso por la presencia de pares clave-valor de etiqueta en la solicitud de ReplicationTask	Cadena

Claves de condición, recursos y acciones de Database Query Metadata Service

Database Query Metadata Service (prefijo de servicio: `dbqms`) proporciona las claves de contexto de condición, acciones y recursos específicas de servicios siguientes para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Database Query Metadata Service
- Tipos de recursos definidos por Database Query Metadata Service
- Claves de condición para Database Query Metadata Service

Acciones definidas por Database Query Metadata Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFavoriteQuery	Otorga permiso para crear una consulta favorita nueva	Write			
CreateQueryHistory	Otorga permiso para agregar una consulta al historial	Write			
CreateTab	Otorga permiso para crear una pestaña de consulta nueva	Write			
DeleteFavoriteQueries	Otorga permiso para eliminar consultas guardadas	Write			
DeleteQueryHistory	Otorga permiso para eliminar una consulta histórica	Write			
DeleteTab	Otorga permiso para eliminar la pestaña de consulta	Write			
DescribeFavoriteQueries	Otorga permiso para mostrar consultas guardadas y metadatos asociados	List			
DescribeQueryHistory	Otorga permiso para mostrar el historial de consultas que se ejecutaron	List			
DescribeTabs	Otorga permiso para mostrar las pestañas de consulta y los metadatos asociados	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueryString	Otorga permiso para recuperar la cadena de consulta favorita o del historial por ID.	Read			
UpdateFavoriteQuery	Otorga permiso para actualizar la consulta y la descripción guardadas	Write			
UpdateQueryHistory	Otorga permiso para actualizar el historial de consultas	Write			
UpdateTab	Otorga permiso para actualizar la pestaña de consulta	Write			

Tipos de recursos definidos por Database Query Metadata Service

Database Query Metadata Service no admite la especificación de un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso al servicio de metadatos de consulta de base de datos, especifique `"Resource": "*"` en la política.

Claves de condición para Database Query Metadata Service

DBQMS no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS DataSync

AWS DataSync (prefijo de servicio:`datasync`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS DataSync
- Tipos de recursos definidos por AWS DataSync
- Claves de condición de AWS DataSync

Acciones definidas por AWS DataSync

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddStorageSystem	Concede permiso para crear un sistema de almacenamiento	Escritura	agent*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CancelTaskExecution	Otorga permiso para cancelar la ejecución de una tarea de sincronización	Write	taskexecution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
CreateAgent	Otorga permiso para activar un agente que haya implementado en el host	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Concede permiso para crear un punto de conexión para un contenedor de Blob Storage de Microsoft Azure	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationEfs	Otorga permiso para crear un punto de enlace para un sistema de archivos de Amazon EFS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxLustre	Otorga permiso para crear un punto de conexión para un Amazon FSx Lustre	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLocationFsxOntap	Concede permiso para crear un punto de conexión para Amazon FSx for ONTAP	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Concede permiso para crear un punto de conexión para Amazon FSx for OpenZFS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxWindows	Otorga permiso para crear un punto final para un sistema de archivos de Amazon FSx Windows File Server	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationHdfs	Otorga permiso para crear un punto de conexión para un Hdfs Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationNfs	Otorga permiso para crear un punto de enlace para un sistema de archivos NFS	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLocationObjectStorage	Otorga permiso para crear un punto de enlace para un bucket de almacenamiento de objetos autoadministrado	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationS3	Otorga permiso para crear un punto de enlace para un bucket de Amazon S3	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationSmb	Otorga permiso para crear un punto de enlace para un sistema de archivos SMB	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTask	Otorga permiso para crear una tarea de sincronización	Escritura	location* agent	 aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Otorga permiso para eliminar un agente	Escritura	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLocation	Otorga permiso para eliminar una ubicación utilizada por AWS DataSync	Escritura	location*		
DeleteTask	Otorga permiso para eliminar una tarea de sincronización	Write	task*		
DescribeAgent	Otorga permiso para ver metadatos, como, por ejemplo, nombre, interfaces de red y estado (es decir, si el agente está o no en ejecución) sobre un agente de sincronización	Lectura	agent*		
DescribeDiscoveryJob	Concede permiso para describir los metadatos de un trabajo de descubrimiento	Lectura	discovery job*		
DescribeLocationAzureBlob	Concede permiso para ver metadatos, como la información de ruta, sobre una ubicación de sincronización de Blob Storage de Azure	Lectura	location*		
DescribeLocationEfs	Otorga permiso para ver metadatos, como, por ejemplo, la información de ruta, sobre una ubicación de sincronización de Amazon EFS	Lectura	location*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeLocationFsxLustre	Otorga permiso para ver los metadatos, como la información de ruta sobre una ubicación de sincronización de Amazon FSx Lustre	Lectura	location*		
DescribeLocationFsxOntap	Otorga permiso para ver los metadatos, como la información de ruta sobre una ubicación de sincronización de Amazon FSx for ONTAP	Lectura	location*		
DescribeLocationFsxOpenZfs	Otorga permiso para ver los metadatos, como la información de ruta sobre una ubicación de sincronización de Amazon FSx OpenZFS	Lectura	location*		
DescribeLocationFsxWindows	Otorga permiso para ver los metadatos, como la información de ruta sobre una ubicación de sincronización de Amazon FSx Windows	Lectura	location*		
DescribeLocationHdfs	Otorga permiso para ver metadatos, como, por ejemplo, la información de ruta sobre una ubicación de sincronización de Amazon HDFS	Lectura	location*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeLocationNfs	Otorga permiso para ver metadatos, como, por ejemplo, la información de ruta, sobre una ubicación de sincronización de NFS	Read	location*		
DescribeLocationObjectStorage	Otorga permiso para ver metadatos sobre una ubicación de servidor de almacenamiento de objetos autoadministrado	Read	location*		
DescribeLocationS3	Otorga permiso para ver metadatos, como, por ejemplo, el nombre del bucket, sobre una ubicación de sincronización de bucket de Amazon S3	Read	location*		
DescribeLocationSmb	Otorga permiso para ver metadatos, como, por ejemplo, la información de ruta, sobre una ubicación de sincronización de SMB	Lectura	location*		
DescribeStorageSystem	Concede permiso para ver los metadatos de un sistema de almacenamiento	Lectura	storagesystem*		
DescribeStorageSystemResourceMetrics	Concede permiso para describir las métricas de recursos recopiladas por un trabajo de descubrimiento	Enumeración	discoveryjob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeStorageSystemResources	Concede permiso para describir los recursos identificados por un trabajo de descubrimiento	Enumeración	discovery job*		
DescribeTask	Concede permiso para ver metadatos sobre una tarea de sincronización	Read	task*		
DescribeTaskExecution	Otorga permiso para ver metadatos sobre una tarea de sincronización que está en ejecución	Lectura	taskexecution*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations	Concede permiso para generar recomendaciones para un recurso identificado por un trabajo de descubrimiento	Escritura	discovery job*		
ListAgents	Otorga permiso para publicar los agentes que son propiedad de una persona Cuenta de AWS en una región especificada en la solicitud	Enumeración			
ListDiscoveryJobs	Concede permiso para enumerar los trabajos de descubrimiento	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLocations	Otorga permiso para enumerar ubicaciones de sincronización de origen y destino	Enumeración			
ListStorageSystems	Concede permiso para enumerar los sistemas de almacenamiento	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas que se han agregado al recurso especificado	Read	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
ListTaskExecutions	Otorga permiso para enumerar las tareas de sincronización ejecutadas	List		aws:ResourceTag/${TagKey}	
ListTasks	Otorga permiso para enumerar todas las tareas de sincronización	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveStorageSystem	Concede permiso para eliminar un sistema de almacenamiento	Escritura	storagesystem*		
StartDiscoveryJob	Concede permiso para iniciar un trabajo de descubrimiento para un sistema de almacenamiento	Escritura	storagesystem*		
StartTaskExecution	Concede permiso para iniciar una invocación específica de una tarea de sincronización	Escritura	task*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	Concede permiso para detener un trabajo de descubrimiento	Escritura	discoveryjob*		
TagResource	Otorga permiso para aplicar un par clave-valor a un recurso AWS	Etiquetado	agent		
			discoveryjob		
			location		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			storagesystem		
			task		
			taskexecution		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una o más etiquetas del recurso especificado.	Etiquetado	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:TagKeys	
UpdateAgent	Otorga permiso para actualizar el nombre de un agente	Escritura	agent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDiscoveryJob	Concede permiso para actualizar un trabajo de descubrimiento	Escritura	discovery job*		
UpdateLocationAzureBlob	Otorga permiso para actualizar una ubicación de sincronización de Blob Storage de Azure	Escritura	location*		
UpdateLocationEfs	Otorga permiso para actualizar una ubicación de sincronización de EFS	Escritura	location*		
UpdateLocationFsxLustre	Otorga permiso para actualizar una ubicación de sincronización de FSx Lustre	Escritura	location*		
UpdateLocationFsxOntap	Otorga permiso para actualizar una ubicación de sincronización de FSx ONTAP	Escritura	location*		
UpdateLocationFsxOpenZfs	Otorga permiso para actualizar una ubicación de sincronización de FSx OpenZFS	Escritura	location*		
UpdateLocationFsxWindows	Otorga permiso para actualizar una ubicación de sincronización de FSx Windows	Escritura	location*		
UpdateLocationHdfs	Otorga permiso para actualizar una ubicación de sincronización de HDFS	Escritura	location*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateLocationNfs	Otorga permiso para actualizar una ubicación de sincronización de NFS	Escritura	location*		
UpdateLocationObjectStorage	Otorga permiso para actualizar una ubicación de servidor de almacenamiento de objetos autoadministrado	Escritura	location*		
UpdateLocationS3	Otorga permiso para actualizar una ubicación de sincronización de S3	Escritura	location*		
UpdateLocationSmb	Otorga permiso para actualizar una ubicación de sincronización de SMB	Escritura	location*		
UpdateStorageSystem	Concede permiso para actualizar una sistema de almacenamiento	Escritura	storagesystem*		
UpdateTask	Otorga permiso para actualizar metadatos asociados a una tarea de sincronización	Write	task*		
UpdateTaskExecution	Otorga permiso para actualizar la ejecución de una tarea de sincronización	Escritura	taskexecution*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS DataSync

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
agent	`arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}`	aws:ResourceTag/${TagKey}
location	`arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}`	aws:ResourceTag/${TagKey}
taskexecution	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}`	aws:ResourceTag/${TagKey}
storagesystem	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}`	aws:ResourceTag/${TagKey}
discoveryjob	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS DataSync

AWS DataSync define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las

que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso en base a los pares de clave-valor de etiqueta asociados con el recurso	Cadena
aws:TagKeys	Filtra las acciones mediante las claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición de Amazon DataZone

Amazon DataZone (prefijo de servicio:`datazone`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon DataZone
- Tipos de recursos definidos por Amazon DataZone
- Claves de estado de Amazon DataZone

Acciones definidas por Amazon DataZone

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptPredictions	Concede permiso para aceptar la predicción	Escritura			
AcceptSubscriptionRequest	Concede permiso para aprobar una solicitud de suscripción para un recurso de datos	Escritura			
AddEntityOwner	Concede permiso para agregar un propietario a una entidad como la unidad de dominio	Escritura			
AddPolicyGrant	Concede permiso para agregar una concesión de política	Administración de permisos			
AssociateEnvironmentRole	Concede permiso para asociar un rol en un entorno de esquema de servicio predeterminado	Escritura			
BatchDeleteLinkedTypes [solo permiso]	Otorga permiso para eliminar elementos de tipo vinculado de un DataZone dominio de Amazon	Escritura	domain*		
BatchPutLinkedType	Otorga permiso para colocar elementos de tipo enlazado	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
s [solo permiso]	en un DataZone dominio de Amazon				
CancelMetadataGenerationRun	Concede permiso para cancelar la ejecución de generación de metadatos	Escritura			
CancelSubscription	Concede permiso para revocar o cancelar la suscripción de una suscripción aprobada a un recurso de datos	Escritura			
CreateAsset	Concede permiso para crear un recurso	Escritura			
CreateAssetFilter	Concede permiso para crear un filtro de activos	Escritura			
CreateAssetRevision	Concede permiso para crear una nueva revisión de un activo	Escritura			
CreateAssetType	Concede permiso para crear un tipo de recurso	Escritura			
CreateConnection	Otorga permiso para crear conexiones	Escritura			
CreateDataProduct	Concede permiso para crear un producto de datos	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataProductRevision	Concede permiso para crear la revisión del producto de datos	Escritura			
CreateDataSource	Otorga permiso para crear una nueva DataSource	Escritura			
CreateDomain	Otorga permiso para aprovisionar un dominio que es una entidad de nivel superior que contiene otros DataZone recursos de Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainUnit	Concede permiso para crear una unidad de dominio	Escritura			
CreateEnvironment	Concede permiso para crear un conjunto de recursos configurados que se utilizan para publicar datos y suscribirse a ellos	Escritura			
CreateEnvironmentAction	Concede permiso para crear una acción de entorno en un entorno de esquema de servicio predeterminado	Escritura			
CreateEnvironmentBlueprint [solo permiso]	Concede permiso para crear un esquema de entorno personalizado que permita al usuario añadir entornos a su proyecto	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironmentProfile	Concede permiso para crear un esquema que se puede utilizar para crear un entorno	Escritura			
CreateFormType	Concede permiso para crear un tipo de formulario o una nueva revisión de este	Escritura			
CreateGlossary	Concede permiso para crear un glosario comercial	Escritura			
CreateGlossaryTerm	Concede permiso para crear un término de glosario	Escritura			
CreateGroupProfile	Otorga permiso para crear un perfil de DataZone grupo para un grupo del IAM Identity Center	Escritura			
CreateListingChangeSet	Concede permiso para crear un conjunto de cambio de lista	Escritura			
CreateProject	Concede permiso para crear un proyecto que permita a su equipo publicar datos y suscribirse a ellos	Escritura			
CreateProjectMembership	Concede permiso para agregar un usuario a un proyecto	Escritura			
CreateProjectProfile	Concede permiso para crear un perfil de proyecto	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRule	Otorga permiso para crear una regla	Escritura			
CreateSubscriptionGrant	Concede permiso para crear una concesión para una suscripción aprobada en un destino de suscripciones	Escritura			
CreateSubscriptionRequest	Concede permiso para crear una solicitud de suscripción para un recurso de datos	Escritura			
CreateSubscriptionTarget	Concede permiso para crear un objetivo de suscripción para un entorno en el proyecto	Escritura			
CreateUserProfile	Concede permiso para crear un perfil de usuario para un usuario existente en el centro de identidades de IAM del cliente	Escritura			
DeleteAsset	Concede permiso para eliminar un activo	Escritura			
DeleteAssetFilter	Concede permiso para eliminar el filtro de activos	Escritura			
DeleteAssetType	Concede permiso para eliminar un tipo de activo	Escritura			
DeleteConnection	Otorga permiso para eliminar conexiones	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDataProduct	Concede permiso para eliminar el producto de datos	Escritura			
DeleteDataSource	Otorga permiso para actualizar las existentes DataSource	Escritura			
DeleteDomain	Concede permiso para eliminar un dominio aprovisionado	Escritura	domain*		
DeleteDomainSharingPolicy [solo permiso]	Otorga permiso para eliminar una política de recursos de un DataZone dominio	Administración de permisos			
DeleteDomainUnit	Concede permiso para eliminar una unidad de dominio existente	Escritura			
DeleteEnvironment	Concede permiso para eliminar un entorno	Escritura			
DeleteEnvironmentAction	Concede permiso para eliminar una acción de entorno en un entorno de esquema de servicio predeterminado	Escritura			
DeleteEnvironmentBlueprint [solo permiso]	Concede permiso para eliminar un esquema de entorno	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEnvironmentBlueprintConfiguration	Concede permiso para eliminar una configuración de esquema de entorno	Escritura			
DeleteEnvironmentProfile	Concede permiso para eliminar un perfil de entorno	Escritura			
DeleteFormType	Concede permiso para eliminar un tipo de formulario	Escritura			
DeleteGlossary	Concede permiso para eliminar un glosario comercial	Escritura			
DeleteGlossaryTerm	Concede permiso para eliminar un término del glosario	Escritura			
DeleteListing	Concede permiso para eliminar una lista	Escritura			
DeleteProject	Concede permiso para eliminar un proyecto que permite a su equipo publicar datos y suscribirse a ellos	Escritura			
DeleteProjectMembership	Concede permiso para eliminar un usuario de un proyecto	Escritura			
DeleteProjectProfile	Concede permiso para eliminar un perfil de proyecto	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRule	Otorga permiso para eliminar una regla	Escritura			
DeleteSubscriptionGrant	Concede permiso para eliminar una concesión para una suscripción en un destino de suscripciones	Escritura			
DeleteSubscriptionRequest	Concede permiso para eliminar una solicitud de suscripción pendiente para un recurso de datos	Escritura			
DeleteSubscriptionTarget	Concede permiso para eliminar un objetivo de suscripción para un entorno en el proyecto	Escritura			
DeleteTimeSeriesDataPoints	Otorga permiso para eliminar una existente TimeSeriesDataPoints	Escritura			
DisassociateEnvironmentRole	Concede permiso para desasociar un rol en un entorno de esquema de servicio predeterminado	Escritura			
GetAsset	Concede permiso para recuperar un recurso	Lectura			
GetAssetFilter	Concede permiso para obtener el filtro de activos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAssetType	Concede permiso para obtener un tipo activo	Lectura			
GetConnection	Otorga permiso para obtener conexiones	Lectura			
GetDataProduct	Concede permiso para obtener el producto de datos	Lectura			
GetDataSource	Otorga permiso para obtener un contenido existente DataSource en Amazon DataZone utilizando su identificador	Lectura			
GetDataSourceRun	Otorga permiso para DataSource ejecutar un trabajo en Amazon DataZone utilizando su identificador	Lectura			
GetDomain	Concede permiso para recuperar información acerca de un dominio	Lectura	domain*		
GetDomainExecutionRoleCredentials [solo permiso]	Otorga permiso para usar funciones que requieren acceso a las credenciales de la función de ejecución del dominio	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDomainSharingPolicy [solo permiso]	Otorga permiso para recuperar una política de recursos para un DataZone dominio	Lectura			
GetDomainUnit	Concede permiso para obtener una unidad de dominio existente	Lectura			
GetEnvironment	Concede permiso para obtener detalles de un entorno	Lectura			
GetEnvironmentAction	Concede permiso para obtener una acción de entorno en un entorno de esquema de servicio predeterminado	Lectura			
GetEnvironmentActionLink [solo permiso]	Concede permiso para obtener un enlace de acción ambiental	Lectura			
GetEnvironmentBlueprint	Concede permiso para obtener los detalles del esquema de entornos	Lectura			
GetEnvironmentBlueprintConfiguration	Concede permiso para obtener la configuración del esquema del entorno	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEnvironmentCredentials	Concede permiso para obtener credenciales a corto plazo que asumen el rol de usuario del entorno	Lectura			
GetEnvironmentProfile	Concede permiso para obtener los detalles del perfil de entorno	Lectura			
GetFormType	Concede permiso para obtener un tipo de formulario	Lectura			
GetGlossary	Concede permiso para obtener un glosario comercial	Lectura			
GetGlossaryTerm	Concede permiso para obtener un término del glosario	Lectura			
GetGroupProfile	Otorga permiso para recuperar un perfil de DataZone grupo existente	Lectura			
GetIamPortalLoginUrl	Otorga permiso a un director de IAM para iniciar sesión en el Portal DataZone	Administración de permisos			
GetJobRun	Otorga permiso para ejecutar trabajos	Lectura			
GetLineageEvent	Otorga permiso para organizar eventos sobre el linaje	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLineageNode	Concede permiso para obtener el nodo de parentesco	Lectura			
GetListing	Concede permiso para obtener una lista	Lectura			
GetMetadataGenerationRun	Concede permiso para ejecutar la generación de metadatos	Lectura			
GetProject	Concede permiso para obtener detalles del proyecto	Lectura			
GetProjectProfile	Concede permiso para obtener detalles del perfil del proyecto	Lectura			
GetRule	Otorga permiso para obtener una regla	Lectura			
GetSubscription	Concede permiso para recuperar una suscripción	Lectura			
GetSubscriptionEligibility [solo permiso]	Concede permiso para obtener elegibilidad de suscripción	Lectura			
GetSubscriptionGrant	Concede permiso para recuperar una concesión de suscripción	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSubscriptionRequestDetails	Concede permiso para rechazar una solicitud de suscripción para un recurso de datos	Lectura			
GetSubscriptionTarget	Concede permiso para recuperar los detalles del objetivo de la suscripción	Lectura			
GetTimeSeriesDataPoint	Otorga permiso para obtener un producto existente TimeSeriesDataPoints en Amazon DataZone utilizando su identificador	Lectura			
GetUpdateEligibility	Otorga permiso para actualizar el estado de aptitud de las construcciones de un proyecto	Lectura			
GetUserProfile	Otorga permiso para recuperar el perfil de un usuario existente en el dominio DataZone	Lectura			
ListAccountEnvironments	Otorga permiso para incluir entornos en todos los dominios de una AWS cuenta	Enumeración			
ListAssetFilters	Concede permiso para enumerar filtros de activos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssetRevisions	Concede permiso para enumerar las revisiones de un activo	Enumeración			
ListConnections	Otorga permiso para enumerar las conexiones	Enumeración			
ListDataProductRevisions	Concede permiso para enumerar las revisiones de los productos de datos	Enumeración			
ListDataSourceRunActivities	Otorga permiso para DataSource enumerar las actividades de un trabajo en Asset	Enumeración			
ListDataSourceRuns	Otorga permiso para enumerar las tareas DataSource ejecutadas	Enumeración			
ListDataSources	Otorga permiso para enumerar las existentes DataSources	Enumeración			
ListDomainUnitsForParent	Concede permiso para enumerar las unidades de dominio secundarias de una unidad de dominio principal determinada	Enumeración			
ListDomains	Concede permiso para recuperar todos los dominios	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntityOwners	Concede permiso para enumerar los propietarios de una entidad como unidad de dominio	Enumeración			
ListEnvironmentActions	Concede permiso para enumerar acciones de entorno en un entorno de proyecto de servicio predeterminado	Enumeración			
ListEnvironmentBlueprintConfigurationSummaries [solo permiso]	Concede permiso para enumerar resúmenes de configuración de esquemas de entorno	Enumeración			
ListEnvironmentBlueprintConfigurations	Concede permiso para enumerar las configuraciones del esquema de entorno	Enumeración			
ListEnvironmentBlueprints	Concede permiso para enumerar un dominio de esquemas	Enumeración			
ListEnvironmentProfiles	Concede permiso para enumerar un dominio para perfiles de entorno	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEnvironments	Concede permiso para mostrar los entornos en el dominio	Enumeración			
ListGroupsForUser	Otorga permiso para enumerar todos los perfiles de DataZone grupo a los que pertenece el perfil de DataZone usuario	Enumeración			
ListJobRuns	Otorga permiso para enumerar las ejecuciones de tareas	Enumeración			
ListLineageEvents	Otorga permiso para enumerar eventos de linaje	Enumeración			
ListLineageNodeHistory	Concede permiso para enumerar las versiones históricas del nodo de parentesco	Enumeración			
ListLinkedTypes [solo permiso]	Otorga permiso para publicar artículos de tipo vinculado a un DataZone dominio de Amazon	Enumeración	domain*		
ListMetadataGenerationRuns	Concede permiso para enumerar ejecuciones de generación de metadatos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNotifications	Concede permiso para enumerar las notificaciones y los eventos para un usuario de DataZone	Enumeración			
ListPolicyGrants	Concede permiso para enumerar concesiones de políticas	Enumeración			
ListProjectMemberships	Concede permiso para enumerar miembros de proyectos	Enumeración			
ListProjectProfiles	Concede permiso para enumerar perfiles de proyectos	Enumeración			
ListProjects	Concede permiso para enumerar proyectos	Enumeración			
ListRules	Otorga permiso para enumerar reglas	Enumeración			
ListSubscriptionGrants	Concede permiso para incluir las concesiones de suscripción a una entidad principal suscrita	Enumeración			
ListSubscriptionRequests	Concede permiso para enumerar las solicitudes de suscripción	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSubscriptionTargets	Concede permiso para enumerar destinos de suscripción	Enumeración			
ListSubscriptions	Concede permiso para enumerar suscripciones	Enumeración			
ListTagsForResource	Concede permiso para recuperar todas las etiquetas asociadas a un recurso	Lectura	domain		
ListTimeSeriesDataPoints	Otorga permiso para incluir las existentes TimeSeriesDataPoints	Enumeración			
ListWarehouseMetadata [solo permiso]	Concede permiso para enumerar los secretos de gerente disponibles.	Enumeración			
PostLineageEvent	Concede permiso para publicar eventos de parentesco	Escritura			
PostTimeSeriesDataPoints	Otorga permiso para publicar una nueva TimeSeriesDataPoints	Escritura			
ProvisionDomain [solo permiso]	Concede permiso para aprovisionar el dominio con la configuración de proyecto predeterminada	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutDomainSharingPolicy [solo permiso]	Otorga permiso para añadir una política de recursos a un DataZone dominio	Administración de permisos			
PutEnvironmentBlueprintConfiguration	Concede permiso para poner la configuración del esquema del entorno	Escritura			
RefreshToken [solo permiso]	Concede permiso para actualizar un token	Escritura			
RejectPredictions	Concede permiso para rechazar la predicción	Escritura			
RejectSubscriptionRequest	Concede permiso para rechazar una solicitud de suscripción para un recurso de datos	Escritura			
RemoveEntityOwner	Concede permiso para eliminar a un propietario existente de una entidad como unidad de dominio	Escritura			
RemovePolicyGrant	Concede permiso para eliminar una concesión de política	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RevokeSubscription	Concede permiso para eliminar una suscripción	Administración de permisos			
Search	Concede permiso para buscar entidades de DataZone	Enumeración			
SearchGroupProfiles	Otorga permiso para buscar perfiles de DataZone grupos y grupos del IAM Identity Center	Enumeración			
SearchListings	Concede permiso para buscar en las listas	Enumeración			
SearchRules [solo permiso]	Otorga permiso para buscar reglas	Enumeración			
SearchTypes	Concede permiso para buscar tipos de activos y formularios en un dominio	Enumeración			
SearchUserProfiles	Otorga permiso para buscar perfiles DataZone de usuario, usuarios del IAM Identity Center y perfiles principales de DataZone IAM	Enumeración			
SsoLogin [solo permiso]	Concede permiso para iniciar sesión mediante el inicio de sesión único	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SsoLogout [solo permiso]	Concede permiso para cerrar sesión como usuario de inicio de sesión único	Escritura			
StartDataSourceRun	Otorga permiso para iniciar un trabajo en ejecución DataSource	Escritura			
StartMetadataGenerationRun	Concede permiso para iniciar una ejecución de generación de metadatos	Escritura			
StopMetadataGenerationRun	Concede permiso para detener la ejecución de generación de metadatos	Escritura			
TagResource	Concede permiso para agregar o actualizar etiquetas en un recurso	Etiquetado	domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas asociadas a un recurso	Etiquetado	domain*		
				aws:TagKeys	
UpdateAssetFilter	Concede permiso para actualizar el filtro de activos	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnection	Otorga permiso para actualizar las conexiones	Escritura			
UpdateDataSource	Otorga permiso para actualizar las existentes DataSource	Escritura			
UpdateDataSourceRunActivities [solo permiso]	Concede permiso para actualizar las actividades de ejecución del origen de datos	Escritura			
UpdateDomain	Concede permiso para actualizar la información de un dominio	Escritura	domain*		
UpdateDomainUnit	Concede permiso para actualizar una unidad de dominio existente	Escritura			
UpdateEnvironment	Concede permiso para actualizar la configuración del entorno	Escritura			
UpdateEnvironmentAction	Concede permiso para actualizar una acción de entorno en un entorno de esquema de servicio predeterminado	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEnvironmentBlueprint [solo permiso]	Concede permiso para actualizar la configuración del esquema de entorno	Escritura			
UpdateEnvironmentConfiguration [solo permiso]	Concede permiso para actualizar la configuración de entorno	Escritura			
UpdateEnvironmentDeploymentStatus [solo permiso]	Concede permiso para actualizar el estado de un entorno	Escritura			
UpdateEnvironmentProfile	Otorga permiso para actualizar EnvironmentProfile la configuración	Escritura			
UpdateGlossary	Concede permiso para actualizar un glosario comercial	Escritura			
UpdateGlossaryTerm	Concede permiso para actualizar un término del glosario	Escritura			
UpdateGroupProfile	Otorga permiso para actualizar el perfil de un DataZone grupo	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateProject	Concede permiso para actualizar un proyecto que permite a su equipo publicar datos y suscribirse a ellos	Escritura			
UpdateProjectProfile	Concede permiso para actualizar un perfil de proyecto	Escritura			
UpdateRule	Otorga permiso para actualizar la regla	Escritura			
UpdateSubscriptionGrantStatus	Concede permiso para actualizar el estado de la concesión de una suscripción para concesiones personalizadas	Escritura			
UpdateSubscriptionRequest	Concede permiso para actualizar el motivo comercial de la solicitud de suscripción de un activo de datos	Escritura			
UpdateSubscriptionTarget	Concede permiso para actualizar un destino de suscripción	Escritura			
UpdateUserProfile	Otorga permiso para actualizar un perfil DataZone de usuario	Escritura			
ValidatePassRole [solo permiso]	Concede permiso para validar roles de paso	Escritura			

Tipos de recursos definidos por Amazon DataZone

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:datazone:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon DataZone

Amazon DataZone define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
datazone:domainId	Filtra el acceso por el ID de dominio introducido en la solicitud	Cadena
datazone:projectId	Filtra el acceso según el ID de proyecto introducido en la solicitud	Cadena
datazone:userId	Filtra el acceso por el ID de usuario introducido en la solicitud	Cadena

Acciones, recursos y claves de condición para AWS Deadline Cloud

AWS Deadline Cloud (prefijo de servicio:`deadline`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Deadline Cloud
- Tipos de recurso definidos por AWS Deadline Cloud
- Claves de condición de AWS Deadline Cloud

Acciones definidas por AWS Deadline Cloud

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateMemberToFarm	Concede permiso para asociar a un miembro a una granja	Administración de permisos	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToFleet	Concede permiso para asociar a un miembro a una flota	Administración de permisos	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:List

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					GroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToJob	Concede permiso para asociar a un miembro a un trabajo	Administración de permisos	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToQueue	Concede permiso para asociar a un miembro a una cola	Administración de permisos	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssumeFleetRoleForRead	Concede permiso para asumir un rol de flota para acceso de solo lectura	Escritura	fleet*		identitystore:ListGroupMembershipsForMember
AssumeFleetRoleForWorker	Concede permiso para asumir un rol de flota para un empleado	Escritura	worker*		
AssumeQueueRoleForRead	Concede permiso para asumir un rol de cola para el acceso de solo lectura	Escritura	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForUser	Concede permiso para asumir un rol de cola para un usuario	Escritura	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForWorker	Concede permiso para asumir un rol de cola para un empleado	Escritura	queue* worker*		
BatchGetJobEntity	Concede permiso para obtener una entidad de trabajo para un empleado	Lectura	worker*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CopyJobTemplate	Concede permiso para copiar una plantilla de trabajo en un bucket de Amazon S3	Escritura	job*		identitystore:ListGroupMembershipsForMember s3:PutObject
CreateBudget	Concede permiso para crear un presupuesto	Escritura	budget*		identitystore:ListGroupMembershipsForMember
CreateFarm	Concede permiso para crear una granja	Escritura	farm*		deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFleet	Otorga permiso para crear una flota.	Escritura	fleet*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Concede permiso para crear un trabajo.	Escritura	job*		deadline:GetJobTemplate identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLicenseEndpoint	Concede permiso para crear un punto de conexión de licencia para software o productos sujetos a licencia	Escritura	license-endpoint*		deadline:TagResource ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLimit	Otorga permiso para crear un límite para una granja	Escritura	farm*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMonitor	Otorga permiso para crear un monitor	Escritura	monitor*		iam:PassRole sso:CreateApplication sso:DeleteApplication sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateQueue	Concede permiso para crear una cola	Escritura	queue*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueueEnvironment	Concede permiso para crear un entorno de cola	Escritura	queue*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateQueueFleetAssociation	Concede permiso para crear una asociación cola-flota	Escritura	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateQueueLimitAssociation	Otorga permiso para crear una asociación con límite de colas	Escritura	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateStorageProfile	Concede permiso para crear un perfil de almacenamiento para una granja	Escritura	farm*		identitystore:ListGroupMembershipsForMember
CreateWorker	Otorga permiso para crear un empleado.	Escritura	worker*		deadline:ListTagsForResource deadline:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBudget	Concede permiso para eliminar un presupuesto	Escritura	budget*		identitystore:ListGroupMembershipsForMember
DeleteFarm	Concede permiso para eliminar una granja	Escritura	farm*		identitystore:ListGroupMembershipsForMember
DeleteFleet	Otorga permiso para eliminar una flota.	Escritura	fleet*		identitystore:ListGroupMembershipsForMember
DeleteLicenseEndpoint	Concede permiso para eliminar un punto de conexión de licencia	Escritura	license-endpoint*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLimit	Otorga permiso para eliminar un límite	Escritura	farm*		identitystore:ListGroupMembershipsForMember
DeleteMeteredProduct	Concede permiso para eliminar un producto medido	Escritura	metered-product*		
DeleteMonitor	Otorga permiso para eliminar un monitor	Escritura	monitor*		sso:DeleteApplication
DeleteQueue	Concede permiso para eliminar una cola	Escritura	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueEnvironment	Concede permiso para eliminar un entorno de cola	Escritura	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueFleetAssociation	Concede permiso para eliminar una asociación cola-flota	Escritura	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteQueueLimitAssociation	Otorga permiso para eliminar una asociación de límite de colas	Escritura	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteStorageProfile	Concede permiso para eliminar un perfil de almacenamiento	Escritura	farm*		identitystore:ListGroupMembershipsForMember
DeleteWorker	Otorga permiso para eliminar un empleado.	Escritura	worker*		
DisassociateMemberFromFarm	Concede permiso para desasociar a un miembro de una granja	Administración de permisos	farm*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromFleet	Concede permiso para desasociar a un miembro de una flota	Administración de permisos	fleet*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromJob	Concede permiso para desasociar a un miembro de un trabajo	Administración de permisos	job*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromQueue	Concede permiso para desasociar a un miembro de una cola	Administración de permisos	queue*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
GetApplicationVersion	Concede permiso para obtener la versión más reciente de una aplicación	Lectura	monitor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBudget	Concede permiso para obtener un presupuesto	Lectura	budget*		identitystore:ListGroupMembershipsForMember
GetFarm	Concede permiso para obtener una granja	Lectura	farm*		identitystore:ListGroupMembershipsForMember
GetFleet	Concede permiso para obtener una flota	Lectura	fleet*		identitystore:ListGroupMembershipsForMember
GetJob	Concede permiso para obtener un trabajo	Lectura	job*		identitystore:ListGroupMembershipsForMember
GetJobTemplate [solo permiso]	Concede permiso para leer la plantilla de trabajo	Lectura	job*		
GetLicenseEndpoint	Concede permiso para obtener un punto de conexión de licencia	Lectura	license-endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLimit	Otorga permiso para obtener un límite	Lectura	farm*		identitystore:ListGroupMembershipsForMember
GetMonitor	Concede permiso para obtener un monitor	Lectura	monitor*		
GetQueue	Concede permiso para obtener una cola	Lectura	queue*		identitystore:ListGroupMembershipsForMember
GetQueueEnvironment	Concede permiso para obtener un entorno de cola	Lectura	queue*		identitystore:ListGroupMembershipsForMember
GetQueueFleetAssociation	Concede permiso para obtener una asociación cola-flota	Lectura	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueueLimitAssociation	Otorga permiso para crear una asociación con límite de colas	Lectura	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
GetSession	Concede permiso para obtener una sesión para un trabajo	Lectura	job*		identitystore:ListGroupMembershipsForMember
GetSessionAction	Concede permiso para obtener una acción de sesión para un trabajo	Lectura	job*		identitystore:ListGroupMembershipsForMember
GetSessionsStatisticsAggregation	Concede permiso para obtener todas las estadísticas recopiladas de las sesiones	Lectura	farm		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetStep	Concede permiso para obtener un paso en un trabajo	Lectura	job*		identitystore:ListGroupMembershipsForMember
GetStorageProfile	Concede permiso para obtener un perfil de almacenamiento	Lectura	farm*		identitystore:ListGroupMembershipsForMember
GetStorageProfileForQueue	Concede permiso para obtener un perfil de almacenamiento de una cola	Lectura	queue*		identitystore:ListGroupMembershipsForMember
GetTask	Concede permiso para obtener una tarea de trabajo	Lectura	job*		identitystore:ListGroupMembershipsForMember
GetWorker	Otorga permiso para obtener un empleado.	Lectura	worker*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAvailableMeteredProducts	Concede permiso para enumerar todos los productos medidos disponibles en un punto de conexión de licencia	Enumeración			
ListBudgets	Concede permiso para enumerar todos los presupuestos de una granja	Enumeración	budget*		identitystore:ListGroupMembershipsForMember
ListFarmMembers	Concede permiso para enumerar todos los miembros de una granja	Enumeración	farm*		identitystore:ListGroupMembershipsForMember
ListFarms	Concede permiso para enumerar todas las granjas	Enumeración	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListFleetMembers	Concede permiso para enumerar todos los miembros de una flota	Enumeración	fleet*		identitystore:ListGroupMembershipsForMember
ListFleets	Otorga permiso para enumerar todas las flotas.	Enumeración	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListJobMembers	Concede permiso para enumerar todos los miembros de un trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember
ListJobParameterDefinitions	Concede permiso para obtener las definiciones de parámetros de un trabajo en la plantilla de trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListJobs	Concede permiso para enumerar todos los trabajos de una cola	Enumeración	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListLicenseEndpoints	Concede permiso para enumerar todos los puntos de conexión de licencia	Enumeración	license-endpoint*		
ListLimits	Otorga permiso para enumerar todos los límites de una granja	Enumeración	farm*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMeteredProducts	Concede permiso para enumerar todos los productos medidos disponibles en un punto de conexión de licencia	Enumeración	metered-product*		
ListMonitors	Concede permiso para enumerar todos los monitores	Enumeración	monitor*		
ListQueueEnvironments	Concede permiso para enumerar todos los entornos de cola a los que una cola está asociada	Enumeración	queue*		identitystore:ListGroupMembershipsForMember
ListQueueFleetAssociations	Concede permiso para enumerar todas las asociaciones cola-flota	Enumeración	farm*		identitystore:ListGroupMembershipsForMember
			fleet*		
			queue*		
ListQueueLimitAssociations	Otorga permiso para enumerar todas las asociaciones con límite de colas	Enumeración	farm*		identitystore:ListGroupMembershipsForMember
			queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQueueMembers	Concede permiso para enumerar todos los miembros de una cola	Enumeración	queue*		identitystore:ListGroupMembershipsForMember
ListQueues	Concede permiso para enumerar todas las colas de una granja	Enumeración	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSessionActions	Concede permiso para enumerar todas las acciones de sesión de un trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember
ListSessions	Concede permiso para enumerar todas las sesiones de un trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember
ListSessionsForWorker	Concede permiso para enumerar todas las sesiones de un empleado	Enumeración	worker*		identitystore:ListGroupMembershipsForMember
ListStepConsumers	Concede permiso para enumerar los consumidores de pasos de un paso de trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember
ListStepDependencies	Concede permiso para enumerar las dependencias de un paso de trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSteps	Concede permiso para enumerar todos los pasos de un trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember
ListStorageProfiles	Concede permiso para enumerar todos los perfiles de almacenamiento de una granja	Enumeración	farm*		identitystore:ListGroupMembershipsForMember
ListStorageProfilesForQueue	Concede permiso para enumerar todos los perfiles de almacenamiento de una cola	Enumeración	queue*		identitystore:ListGroupMembershipsForMember
ListTagsForResource	Concede permiso para enumerar todas las etiquetas de recursos especificados de Deadline Cloud	Enumeración	farm		
			fleet		
			license-endpoint		
			queue		
			worker		
				deadline:CalledAction	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTasks	Concede permiso para enumerar todas las tareas de un trabajo	Enumeración	job*		identitystore:ListGroupMembershipsForMember
ListWorkers	Concede permiso para enumerar todos los empleados de una flota	Enumeración	worker*		identitystore:ListGroupMembershipsForMember
PutMeteredProduct	Concede permiso para agregar un producto medido a un punto de conexión de licencia	Escritura	metered-product*		
SearchJobs	Concede permiso para buscar trabajos en varias colas	Enumeración	queue*		identitystore:ListGroupMembershipsForMember
SearchSteps	Concede permiso para buscar los pasos dentro de un único trabajo o para buscar los pasos de varias colas	Enumeración	job		identitystore:ListGroupMembershipsForMember
			queue		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchTasks	Concede permiso para buscar las tareas dentro de un único trabajo o para buscar las tareas de varias colas	Enumeración	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchWorkers	Concede permiso para buscar empleados en varias flotas	Enumeración	fleet*		identitystore:ListGroupMembershipsForMember
StartSessionsStatisticsAggregation	Concede permiso para obtener todas las estadísticas recopiladas de las sesiones	Lectura	fleet		identitystore:ListGroupMembershipsForMember
			queue		
TagResource	Concede permiso para agregar o sobrescribir una o más etiquetas para el recurso especificado de Deadline Cloud	Etiquetado	farm		
			fleet		
			license-endpoint		
			queue		
			worker		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys deadline:CalledAction	
UntagResource	Concede permiso para desasociar una o más etiquetas del recurso de Deadline Cloud especificado	Etiquetado	farm		
			fleet		
			license-endpoint		
			queue		
			worker		
				aws:TagKeys	
UpdateBudget	Autorización para actualizar un presupuesto	Escritura	budget*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFarm	Concede permiso para actualizar una granja	Escritura	farm*		identitystore:ListGroupMembershipsForMember
UpdateFleet	Concede permiso para actualizar una flota	Escritura	fleet*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateJob	Concede permiso para actualizar un trabajo.	Escritura	job*		identitystore:ListGroupMembershipsForMember
UpdateLimit	Otorga permiso para actualizar el límite de una granja	Escritura	farm*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMonitor	Otorga permiso para actualizar un monitor	Escritura	monitor*		iam:PassRole sso:PutApplicationGrant sso:UpdateApplication
UpdateQueue	Concede permiso para actualizar una cola	Escritura	queue*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateQueueEnvironment	Concede permiso para actualizar un entorno de cola	Escritura	queue*		identitystore:ListGroupMembershipsForMember
UpdateQueueFleetAssociation	Concede permiso para actualizar una asociación cola-flota	Escritura	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQueueLimitAssociation	Otorga permiso para actualizar una asociación con límites de colas	Escritura	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateSession	Concede permiso para actualizar una sesión de un trabajo	Escritura	job*		identitystore:ListGroupMembershipsForMember
UpdateStep	Concede permiso para actualizar un paso de un trabajo	Escritura	job*		identitystore:ListGroupMembershipsForMember
UpdateStorageProfile	Concede permiso para actualizar un perfil de almacenamiento de una granja	Escritura	farm*		identitystore:ListGroupMembershipsForMember
UpdateTask	Otorga permiso para actualizar una tarea.	Escritura	job*		identitystore:ListGroupMembershipsForMember

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateWorker	Concede permiso para actualizar un empleado.	Escritura	worker*		logs:CreateLogStream
UpdateWorkerSchedule	Concede permiso para actualizar la programación de un empleado	Escritura	worker*		logs:CreateLogStream

Tipos de recurso definidos por AWS Deadline Cloud

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
budget	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/budget/${BudgetId}`	deadline:FarmMembershipLevels
farm	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels

Tipos de recurso	ARN	Claves de condición
fleet	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels
job	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}/job/${JobId}	deadline:FarmMembershipLevels deadline:JobMembershipLevels deadline:QueueMembershipLevels
license-endpoint	arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}	aws:ResourceTag/${TagKey}
metered-product	arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}/metered-product/${ProductId}	
monitor	arn:${Partition}:deadline:${Region}:${Account}:monitor/${MonitorId}	

Tipos de recurso	ARN	Claves de condición
queue	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:QueueMembershipLevels
worker	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}/worker/${WorkerId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels

Claves de condición de AWS Deadline Cloud

AWS Deadline Cloud define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
deadline:AssociatedMembershipLevel	Filtra el acceso por el nivel de membresía asociado de la entidad principal proporcionada en la solicitud	Cadena
deadline:CalledAction	Filtra el acceso según la acción permitida en la solicitud	Cadena
deadline:FarmMembershipLevels	Filtra el acceso por niveles de membresía en la granja	ArrayOfString
deadline:FleetMembershipLevels	Filtra el acceso por niveles de membresía en la flota	ArrayOfString
deadline:JobMembershipLevels	Filtra el acceso por niveles de membresía en el trabajo	ArrayOfString
deadline:MembershipLevel	Filtra el acceso según el nivel de membresía transmitido en la solicitud	Cadena
deadline:PrincipalId	Filtra el acceso por el ID de entidad principal proporcionado en la solicitud	Cadena

Claves de condición	Descripción	Tipo
deadline:QueueMembershipLevels	Filtra el acceso por niveles de membresía en la cola	ArrayOfString
deadline:RequesterPrincipalId	Filtra el acceso por el usuario que llama a la API de Deadline Cloud	Cadena

Acciones, recursos y claves de condición para AWS DeepComposer

AWS DeepComposer (prefijo de servicio:`deepcomposer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS DeepComposer
- Tipos de recursos definidos por AWS DeepComposer
- Claves de condición de AWS DeepComposer

Acciones definidas por AWS DeepComposer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateCoupon [solo permiso]	Otorga permiso para asociar un DeepComposer cupón (o DSN) a la cuenta asociada al remitente de la solicitud	Escritura			
CreateAudio [solo permiso]	Concede permiso para crear un archivo de audio convirtiendo la composición midi en un archivo wav o mp3	Write	audio*		
CreateComposition [solo permiso]	Concede permiso para crear una composición midi de varias pistas	Write	composition*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel [solo permiso]	Concede permiso para iniciar creating/training un modelo generativo que es capaz de realizar inferencias a partir de la melodía de piano proporcionada por el usuario para crear una composición midi multipista	Escritura	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComposition [solo permiso]	Concede permiso para eliminar la composición	Write	composition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteModel	Concede permiso para eliminar el modelo	Write	model*		
GetComposition [solo permiso]	Concede permiso para obtener información acerca de la composición	Read	composition*		
				aws:ResourceTag/${TagKey}	
GetModel [solo permiso]	Concede permiso para obtener información acerca del modelo	Read	model*		
				aws:ResourceTag/${TagKey}	
GetSampleModel [solo permiso]	Otorga permiso para obtener información sobre la muestra o el modelo previamente entrenado DeepComposer	Lectura	model*		
ListCompositions [solo permiso]	Concede permiso para enumerar todas las composiciones propiedad del remitente de la solicitud	List	composition*		
ListModels [solo permiso]	Concede permiso para enumerar todos los modelos propiedad del remitente de la solicitud	List	model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSampleModels [solo permiso]	Otorga permiso para enumerar todos los modelos de muestra o preentrenados proporcionados por el servicio DeepComposer	Enumeración	model*		
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	List	composition		
			model		
				aws:ResourceTag/${TagKey}	
ListTrainingTopics [solo permiso]	Otorga permiso para enumerar todas las opciones o temas de formación de un modelo creating/training	Enumeración	model*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	composition		
			model		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	composition		
			model		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateComposition [solo permiso]	Concede permiso para modificar las propiedades mutables asociadas a una composición	Write	composition*		
UpdateModel [solo permiso]	Concede permiso para modificar las propiedades mutables asociadas a un modelo	Escritura	model*		

Tipos de recursos definidos por AWS DeepComposer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
model	`arn:${Partition}:deepcomposer:${Region}:${Account}:model/${ModelId}`	aws:ResourceTag/${TagKey}
composition	`arn:${Partition}:deepcomposer:${Region}:${Account}:composition/${CompositionId}`	aws:ResourceTag/${TagKey}
audio	`arn:${Partition}:deepcomposer:${Region}:${Account}:audio/${AudioId}`	

Claves de condición de AWS DeepComposer

AWS DeepComposer define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante acciones en función de pares de clave-valor asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante acciones en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS DeepRacer

AWS DeepRacer (prefijo de servicio:`deepracer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS DeepRacer
- Tipos de recursos definidos por AWS DeepRacer
- Claves de condición de AWS DeepRacer

Acciones definidas por AWS DeepRacer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddLeaderboardAccessPermission [solo permiso]	Concede permiso para agregar acceso a una tabla de clasificación privada	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
AdminDescribeAccountKey [solo permiso]	Otorga permiso para recuperar la información de la clave KMS que el usuario ha asignado actualmente a su cuenta	Lectura		deepracer:UserToken deepracer:MultiUser	
AdminGetAccountConfig [solo permiso]	Concede permiso para obtener la configuración actual de multiusuario de administrador para esta cuenta	Lectura			
AdminListAssociatedResources [solo permiso]	Concede permiso para enumerar todos los usuarios DeepRacer con sus recursos asociados creados bajo esta cuenta	Lectura			
AdminListAssociate	Concede permiso para enumerar los datos de	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
dUsers [solo permiso]	usuario de todos los usuarios asociados a esta cuenta				
AdminManageUser [solo permiso]	Concede permiso para administrar un usuario asociado a esta cuenta	Escritura			
AdminSetAccountConfig [solo permiso]	Concede permiso para establecer opciones de configuración para esta cuenta	Escritura			
AdminUpdateAccountKey [solo permiso]	Otorga permiso para actualizar la clave KMS asignada a la cuenta del usuario	Escritura		deepracer:UserToken deepracer:MultiUser	
CloneReinforcementLearningModel [solo permiso]	Otorga permiso para clonar un DeepRacer modelo existente	Escritura	reinforcement_learning_model* track*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateCar [solo permiso]	Otorga permiso para crear un DeepRacer coche en tu garaje	Escritura		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLeaderboard [solo permiso]	Concede permiso para crear una tabla de clasificación	Write		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateLeaderboardAccessToken [solo permiso]	Concede permiso para crear un token de acceso a una tabla de clasificación privada	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
CreateLeaderboardSubmission [solo permiso]	Otorga permiso para enviar un DeepRacer modelo para que lo evalúen en las tablas de clasificación	Escritura	leaderboard*		
			reinforcement_learning_model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateReinforcementLearningModel [solo permiso]	Otorga permiso para crear un modelo de aprendizaje reforzado para DeepRacer	Escritura	track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLeaderboard [solo permiso]	Concede permiso para eliminar una tabla de clasificación	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
DeleteModel [solo permiso]	Otorga permiso para eliminar un modelo DeepRacer	Escritura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
EditLeaderboard [solo permiso]	Concede permiso para editar una tabla de clasificación	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountConfig [solo permiso]	Concede permiso para obtener la configuración actual de multiusuario para esta cuenta	Lectura		deepracer:UserToken deepracer:MultiUser	
GetAlias [solo permiso]	Otorga permiso para recuperar el alias del usuario para enviar un DeepRacer modelo a las tablas de clasificación	Lectura		deepracer:UserToken deepracer:MultiUser	
GetAssetUrl [solo permiso]	Otorga permiso para descargar artefactos de un modelo existente DeepRacer	Lectura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
GetCar [solo permiso]	Otorga permiso para recuperar un DeepRacer coche específico de tu garaje	Lectura	car*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deepracer:UserToken deepracer:MultiUser	
GetCars [solo permiso]	Otorga permiso para ver todos los DeepRacer coches de tu garaje	Lectura		deepracer:UserToken deepracer:MultiUser	
GetEvaluation [solo permiso]	Otorga permiso para recuperar información sobre las tareas de evaluación de un DeepRacer modelo existente	Lectura	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLatestUserSubmission [solo permiso]	Otorga permiso para recuperar información sobre el rendimiento del último DeepRacer modelo presentado por un usuario en una tabla de clasificación	Lectura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetLeaderboard [solo permiso]	Concede permiso para recuperar información acerca de tablas de clasificación.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetModel [solo permiso]	Otorga permiso para recuperar información sobre un modelo existente DeepRacer	Lectura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPrivateLeaderboard [solo permiso]	Concede permiso para recuperar información acerca de tablas de clasificación privadas	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetRankedUserSubmission [solo permiso]	Otorga permiso para recuperar información sobre el rendimiento del DeepRacer modelo de un usuario que se ubicó en una tabla de clasificación	Lectura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetTrack [solo permiso]	Otorga permiso para recuperar información sobre las pistas DeepRacer	Lectura	track*		
GetTrainingJob [solo permiso]	Otorga permiso para recuperar información sobre el trabajo de formación de un DeepRacer modelo existente	Lectura	training_job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deepracer:UserToken deepracer:MultiUser	
ImportModel [solo permiso]	Otorga permiso para importar un modelo de aprendizaje por refuerzo para DeepRacer	Escritura		deepracer:UserToken deepracer:MultiUser	
ListEvaluations [solo permiso]	Otorga permiso para enumerar los trabajos de evaluación de un DeepRacer modelo	Lectura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardEvaluations [solo permiso]	Concede permiso para enumerar todos los trabajos de evaluación de clasificación de un usuario para una tabla de clasificación	Lectura	leaderboard*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardSubmissions [solo permiso]	Otorga permiso para incluir todos los DeepRacer modelos presentados por un usuario en una tabla de clasificación	Lectura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboards [solo permiso]	Concede permiso para enumerar todas las tablas de clasificación disponibles.	Read		deepracer:UserToken deepracer:MultiUser	
ListModels [solo permiso]	Otorga permiso para enumerar todos los modelos existentes DeepRacer	Lectura		deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPrivateLeaderboardParticipants [solo permiso]	Concede permiso para recuperar información del participante acerca de tablas de clasificación privadas	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboards [solo permiso]	Concede permiso para enumerar todas las tablas de clasificación privadas disponibles	Read		deepracer:UserToken deepracer:MultiUser	
ListSubscribedPrivateLeaderboards [solo permiso]	Concede permiso para enumerar todas las tablas de clasificación privadas suscritas	Lectura		deepracer:UserToken deepracer:MultiUser	
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso	Lectura	car		
			evaluation_job		
			leaderboard		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		
				aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
ListTracks [solo permiso]	Otorga permiso para enumerar todas las DeepRacer pistas	Lectura			
ListTrainingJobs [solo permiso]	Otorga permiso para enumerar los trabajos de entrenamiento de una DeepRacer modelo	Lectura	reinforcement_learning_model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deepracer:UserToken deepracer:MultiUser	
MigrateModels [solo permiso]	Otorga permiso para migrar modelos de aprendizaje por refuerzo anteriores para DeepRacer	Escritura			
PerformLeaderboardOperation [solo permiso]	Concede permiso para realizar la operación de tabla de clasificación mencionada en el atributo de operación	Escritura	leaderboard		
				deepracer:UserToken deepracer:MultiUser	
RemoveLeaderboardAccessPermission [solo permiso]	Concede permiso para quitar el acceso a una tabla de clasificación privada	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetAlias [solo permiso]	Otorga permiso para establecer el alias del usuario para enviar un DeepRacer modelo a las tablas de clasificación	Escritura		deepracer:UserToken deepracer:MultiUser	
StartEvaluation [solo permiso]	Otorga permiso para evaluar un DeepRacer modelo en un entorno simulado	Escritura	reinforcement_learning_model*		
			track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
StopEvaluation [solo permiso]	Otorga permiso para detener las evaluaciones DeepRacer del modelo	Escritura	evaluation_job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deepracer:UserToken deepracer:MultiUser	
StopTrainingReinforcementLearningModel [solo permiso]	Otorga permiso para dejar de entrenar a un DeepRacer modelo	Escritura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			reinforcement_learning_model		
			training_job		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
TestRewardFunction [solo permiso]	Concede permiso para probar la corrección de las funciones de recompensa.	Escritura			
UntagResource		Etiquetado	car		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para eliminar etiquetas en un recurso		evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		
				aws:TagKeys deepracer:UserToken deepracer:MultiUser	
UpdateCar [solo permiso]	Otorga permiso para actualizar un DeepRacer coche en tu garaje	Escritura	car*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				deepracer:UserToken deepracer:MultiUser	

Tipos de recursos definidos por AWS DeepRacer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
car	`arn:${Partition}:deepracer:${Region}:${Account}:car/${ResourceId}`	aws:ResourceTag/${TagKey}
evaluation_job	`arn:${Partition}:deepracer:${Region}:${Account}:evaluation_job/${ResourceId}`	aws:ResourceTag/${TagKey}
leaderboard	`arn:${Partition}:deepracer:${Region}::leaderboard/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
leaderboard_evaluation_job	arn:${Partition}:deepracer:${Region}:${Account}:leaderboard_evaluation_job/${ResourceId}	aws:ResourceTag/${TagKey}
reinforcement_learning_model	arn:${Partition}:deepracer:${Region}:${Account}:model/reinforcement_learning/${ResourceId}	aws:ResourceTag/${TagKey}
track	arn:${Partition}:deepracer:${Region}::track/${ResourceId}	
training_job	arn:${Partition}:deepracer:${Region}:${Account}:training_job/${ResourceId}	aws:ResourceTag/${TagKey}

Claves de condición de AWS DeepRacer

AWS DeepRacer define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString
deepracer:MultiUser	Filtra el acceso por indicador multiusuario	Bool
deepracer:UserToken	Filtra el acceso por token de usuario en la solicitud	Cadena

Acciones, recursos y claves de condición de Amazon Detective

Amazon Detective (prefijo de servicio: `detective`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Detective
- Tipos de recurso definidos por Amazon Detective
- Claves de condición de Amazon Detective

Acciones definidas por Amazon Detective

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptInvitation	Concede permiso para aceptar una invitación para convertirse en miembro de un gráfico de comportamiento.	Escritura	Graph*		
BatchGetGraphMemberDatasources	Concede permiso para recuperar el historial del paquete de origen de datos de la cuenta de miembro especificada en un gráfico de comportamiento administrado por esta cuenta	Lectura	Graph*		
BatchGetMembershipDatasources	Concede permiso para recuperar el historial del paquete de origen de datos de la cuenta de la persona que llama para los gráficos especificados	Lectura			
CreateGraph	Concede permiso para crear un gráfico de comportamiento y comenzar a agregar información de seguridad.	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	detective:TagResource
CreateMembers	Concede permiso para solicitar la pertenencia a una o	Write	Graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	más cuentas en un gráfico de comportamiento administrado por esta cuenta.				
DeleteGraph	Concede permiso para eliminar un gráfico de comportamiento y dejar de agregar información de seguridad.	Write	Graph*		
DeleteMembers	Concede permiso para quitar cuentas de miembro de un gráfico de comportamiento administrado por esta cuenta.	Escritura	Graph*		
DescribeOrganizationConfiguration	Otorga permiso para ver la configuración actual relacionada con la integración de Amazon Detective con AWS Organizations	Lectura	Graph*		organizations:DescribeOrganization
DisableOrganizationAdminAccount	Concede permiso para eliminar la cuenta de administrador delegado de Amazon Detective para una organización	Escritura			organizations:DescribeOrganization
DisassociateMembership	Concede permiso para eliminar la asociación de esta cuenta con un gráfico de comportamiento.	Escritura	Graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableOrganizationAdminAccount	Concede permiso para designar la cuenta de administrador delegado de Amazon Detective para una organización	Escritura			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
GetFreeTrialEligibility [solo permiso]	Concede permiso para recuperar la elegibilidad de un gráfico de comportamiento para un periodo de prueba gratuita.	Read	Graph*		
GetGraphIngestState [solo permiso]	Concede permiso para obtener el estado de ingestión de datos de un gráfico de comportamiento.	Lectura	Graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetInvestigation	Concede permiso para obtener el estado y los metadatos de una investigación	Lectura	Graph*		
GetMembers	Concede permiso para obtener detalles de miembros específicos de un gráfico de comportamiento.	Read	Graph*		
GetPricingInformation [solo permiso]	Concede permiso para obtener información sobre los precios de Amazon Detective.	Read			
GetUsageInformation [solo permiso]	Concede permiso para enumerar la información de uso de un gráfico de comportamiento.	Lectura	Graph*		
InvokeAssistant [solo permiso]	Concede permiso para invocar al asistente de Detective	Lectura	Graph*		
ListDatasourcePackages	Concede permiso para enumerar los estados de ingesta del paquete de origen de datos de un gráfico y las marcas de tiempo para los cambios de estado más recientes en un gráfico de comportamiento administrado por esta cuenta	Enumeración	Graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGraphs	Concede permiso para enumerar los gráficos de comportamiento administrados por esta cuenta.	Enumeración			
ListHighDegreeEntities [solo permiso]	Otorga permiso para recuperar entidades de gran volumen cuyas relaciones no pueda almacenar Detective	Enumeración	Graph*		
ListIndicators	Concede permiso para enumerar los indicadores de una investigación	Enumeración	Graph*		
ListInvestigations	Concede permiso para enumerar las investigaciones de un gráfico de comportamiento	Enumeración	Graph*		
ListInvitations	Concede permiso para obtener detalles sobre los gráficos de comportamiento a los que se ha invitado a unirse a esta cuenta.	List			
ListMembers	Concede permiso para obtener detalles de todos los miembros de un gráfico de comportamiento.	Enumeración	Graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOrganizationAdminAccount	Concede permiso para ver la cuenta de administrador delegado de Amazon Detective para una organización	Enumeración			organizations:DescribeOrganization
ListTagsForResource	Concede permiso para mostrar los valores de etiqueta asignados a un gráfico de comportamiento	Enumeración	Graph*		
				aws:ResourceTag/${TagKey}	
RejectInvitation	Concede permiso para rechazar una invitación para convertirse en miembro de un gráfico de comportamiento.	Write	Graph*		
SearchGraph [solo permiso]	Concede permiso para buscar los datos almacenados en un gráfico de comportamiento.	Lectura	Graph*		
StartInvestigation	Concede permiso para iniciar investigaciones	Escritura	Graph*		
StartMonitoringMember	Concede permiso para iniciar la captura de datos para una cuenta de miembro que tiene el estado ACCEPTED_BUT_DISABLED	Escritura	Graph*		
TagResource	Concede permiso para asignar valores de etiqueta a un gráfico de comportamiento	Etiquetado	Graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar valores de etiqueta de un gráfico de comportamiento	Etiquetado	Graph*		
				aws:TagKeys	
UpdateDatasourcePackages	Concede permiso para habilitar o deshabilitar un paquete o paquetes de origen de datos en un gráfico de comportamiento administrado por esta cuenta	Escritura	Graph*		
UpdateInvestigationState	Concede permiso para actualizar el estado y los metadatos de una investigación	Escritura	Graph*		
UpdateOrganizationConfiguration	Otorga permiso para actualizar la configuración actual relacionada con la integración de Amazon Detective con AWS Organizations	Escritura	Graph*		organizations:DescribeOrganization

Tipos de recurso definidos por Amazon Detective

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Graph	`arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Detective

Amazon Detective define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso especificando las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso especificando las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso especificando las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Device Farm

AWS Device Farm (prefijo de servicio:`devicefarm`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Device Farm
- Tipos de recursos definidos por AWS Device Farm
- Claves de condición para AWS Device Farm

Acciones definidas por AWS Device Farm

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDevicePool	Otorga permiso para crear un grupo de dispositivos dentro de un proyecto.	Write	project*		
CreateInstanceProfile	Otorga permiso para crear un nuevo perfil de instancia de dispositivo.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNetworkProfile	Otorga permiso para crear un perfil de red dentro de un proyecto.	Write	project*		
CreateProject	Otorga permiso para crear un proyecto para probarlo en un móvil.	Escritura			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateRemoteAccessSession	Otorga permiso para iniciar una sesión de acceso remoto a una instancia de dispositivo.	Write	device*		
			project*		
			deviceinstance		
			upload		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTestGridProject	Otorga permiso para crear un proyecto para probarlo en el escritorio	Write			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateTestGridUrl	Otorga permiso para generar una nueva URL previamente firmada utilizada para acceder a nuestro servicio de matriz de pruebas.	Write	testgrid-project*		
CreateUpload	Otorga permiso para cargar un nuevo archivo o aplicación dentro de un proyecto.	Write	project*		
CreateVPCEConfiguration	Otorga permiso para crear una configuración de punto de enlace de Amazon Virtual Private Cloud (VPC).	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDevicePool	Otorga permiso para eliminar un grupo de dispositivos generado por el usuario.	Write	devicepool*		
DeleteInstanceProfile	Otorga permiso para eliminar un perfil de instancia generado por el usuario.	Write	instanceprofile*		
DeleteNetworkProfile	Otorga permiso para eliminar un perfil de red generado por el usuario.	Write	networkprofile*		
DeleteProject	Otorga permiso para eliminar un proyecto de prueba en el móvil.	Write	project*		
DeleteRemoteAccessSession	Otorga permiso para eliminar una sesión de acceso remoto completada y sus resultados.	Write	session*		
DeleteRun	Otorga permiso para eliminar una ejecución.	Write	run*		
DeleteTestGridProject	Otorga permiso para eliminar un proyecto de prueba en el escritorio.	Write	testgrid-project*		
DeleteUpload	Otorga permiso para eliminar un archivo cargado por el usuario.	Write	upload*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteVPCEConfiguration	Otorga permiso para eliminar una configuración de punto de enlace de Amazon Virtual Private Cloud (VPC).	Escritura	vpceconfiguration*		
GetAccountSettings	Otorga permiso para recuperar el número de dispositivos iOS no medidos y Android and/or comprados por la cuenta	Lectura			
GetDevice	Otorga permiso para recuperar la información de un tipo de dispositivo único.	Read	device*		
GetDeviceInstance	Otorga permiso para retirar la información de una instancia de dispositivo.	Read	deviceinstance*		
GetDevicePool	Otorga permiso para retirar la información de un grupo de dispositivos.	Lectura	devicepool*		
GetDevicePoolCompatibility	Otorga permiso para recuperar información sobre la compatibilidad de una and/or aplicación de prueba con un grupo de dispositivos	Lectura	devicepool* upload		
GetInstanceProfile	Otorga permiso para retirar la información de un perfil de instancia.	Read	instanceprofile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetJob	Otorga permiso para retirar la información de un trabajo.	Read	job*		
GetNetworkProfile	Otorga permiso para retirar la información de un perfil de red.	Lectura	networkprofile*		
GetOfferingStatus	Otorga permiso para recuperar el estado actual y futuro de todas las ofertas adquiridas por un Cuenta de AWS	Lectura			
GetProject	Otorga permiso para recuperar información sobre un proyecto de prueba en el móvil.	Read	project*		
GetRemoteAccessSession	Otorga permiso para retirar el enlace a una sesión de acceso remoto que se está ejecutando actualmente.	Read	session*		
GetRun	Otorga permiso para retirar la información de una ejecución.	Read	run*		
GetSuite	Otorga permiso para retirar la información de un conjunto de pruebas.	Read	suite*		
GetTest	Otorga permiso para retirar la información de un caso de prueba.	Read	test*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTestGridProject	Otorga permiso para recuperar información sobre un proyecto de prueba en el escritorio.	Read	testgrid-project*		
GetTestGridSession	Otorga permiso para retirar la información de un sesión de matriz de pruebas.	Read	testgrid-project		
			testgrid-session		
GetUpload	Otorga permiso para retirar la información de un archivo cargado.	Read	upload*		
GetVPCEConfiguration	Otorga permiso para retirar la información de una configuración de punto de enlace de Amazon Virtual Private Cloud (VPC).	Read	vpceconfiguration*		
InstallToRemoteAccessSession	Otorga permiso para instalar una aplicación en un dispositivo en una sesión de acceso remoto.	Write	session*		
			upload*		
ListArtifacts	Otorga permiso para enumerar los artefactos de un proyecto.	List	job		
			run		
			suite		
			test		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeviceInstances	Otorga permiso para mostrar la información de las instancias de dispositivo.	List			
ListDevicePools	Otorga permiso para mostrar la información de los grupos de dispositivos.	List	project*		
ListDevices	Otorga permiso para mostrar la información de tipos de dispositivos únicos.	List			
ListInstanceProfiles	Otorga permiso para mostrar la información de los perfiles de instancia de dispositivo.	List			
ListJobs	Otorga permiso para mostrar la información de los trabajos dentro de una ejecución.	List	run*		
ListNetworkProfiles	Otorga permiso para mostrar la información de perfiles de red dentro de un proyecto.	List	project*		
ListOfferingPromotions	Otorga permiso para publicar las promociones de la oferta.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOfferingTransactions	Otorga permiso para enumerar todo el historial de compras, renovaciones y transacciones de renovación del sistema de un Cuenta de AWS	Enumeración			
ListOfferings	Otorga permiso para mostrar la lista de los productos u ofertas que el usuario puede administrar a través de la API.	Enumeración			
ListProjects	Otorga permiso para incluir la información de los proyectos de pruebas móviles para un Cuenta de AWS	Enumeración			
ListRemoteAccessSessions	Otorga permiso para mostrar la información de las sesiones de acceso remoto que se están ejecutando actualmente.	List	project*		
ListRuns	Otorga permiso para mostrar la información de las ejecuciones dentro de un proyecto.	List	project*		
ListSamples	Otorga permiso para mostrar la información de muestras dentro de un proyecto.	List	job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSuites	Otorga permiso para mostrar la información de los conjuntos de pruebas dentro de un trabajo.	List	job*		
ListTagsForResource	Otorga permiso para obtener una lista de las etiquetas de un recurso.	Enumeración	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTestGridProjects	Otorga permiso para incluir la información de los proyectos de pruebas de escritorio para un Cuenta de AWS	Enumeración			
ListTestGridSessionActions	Otorga permiso para mostrar las acciones de la sesión realizadas durante una sesión de matriz de pruebas.	List	testgrid-session*		
ListTestGridSessionArtifacts	Otorga permiso para mostrar los artefactos generados por una sesión de matriz de pruebas.	List	testgrid-session*		
ListTestGridSessions	Otorga permiso para mostrar las sesiones dentro de un proyecto de matriz de pruebas.	List	testgrid-project*		
ListTests	Otorga permiso para enumerar la información de las pruebas dentro de un conjunto de pruebas.	List	suite*		
ListUniqueProblems	Otorga permiso para mostrar la información de problemas únicos dentro de una ejecución.	List	run*		
ListUploads	Otorga permiso para mostrar la información de las cargas dentro de un proyecto.	List	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListVPCEConfigurations	Otorga permiso para mostrar la información de las configuraciones de punto de enlace de Amazon Virtual Private Cloud (VPC).	Enumeración			
PurchaseOffering	Otorga permiso para comprar ofertas para un Cuenta de AWS	Escritura			
RenewOffering	Otorga permiso para establecer la cantidad de dispositivos que se van a renovar para una oferta.	Write			
ScheduleRun	Otorga permiso para programar una ejecución.	Write	project* devicepool upload		
	ESCENARIO: Device Pool as filter		devicepool* project* upload		
	ESCENARIO: Device Selection Configuration as filter		project* upload		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopJob	Otorga permiso para terminar un trabajo en ejecución.	Write	job*		
StopRemoteAccessSession	Otorga permiso para terminar una sesión de acceso remoto en ejecución.	Write	session*		
StopRun	Otorga permiso para terminar una ejecución de prueba en ejecución.	Write	run*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			testgrid-session		
			vpceconfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			testgrid-session		
			vpceconfiguration		
				aws:TagKeys	
UpdateDeviceInstance	Otorga permiso para modificar una instancia de dispositivo existente.	Write	deviceinstance*		
			instanceprofile		
UpdateDevicePool	Otorga permiso para modificar un grupo de dispositivos existente.	Write	devicepool*		
UpdateInstanceProfile	Otorga permiso para modificar un perfil de instancia existente.	Write	instanceprofile*		
UpdateNetworkProfile	Otorga permiso para modificar un perfil de red existente.	Write	networkprofile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateProject	Otorga permiso para modificar un proyecto de prueba en el móvil existente.	Write	project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTestGridProject	Otorga permiso para modificar un proyecto de prueba en el escritorio existente.	Write	testgrid-project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	Otorga permiso para modificar una carga existente.	Write	upload*		
UpdateVPCEConfiguration	Otorga permiso para modificar una configuración de punto de enlace de Amazon Virtual Private Cloud (VPC) existente.	Write	vpceconfiguration*		

Tipos de recursos definidos por AWS Device Farm

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
project	arn:${Partition}:devicefarm:${Region}:${Account}:project:${ResourceId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:devicefarm:${Region}:${Account}:run:${ResourceId}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:devicefarm:${Region}:${Account}:job:${ResourceId}	
suite	arn:${Partition}:devicefarm:${Region}:${Account}:suite:${ResourceId}	
test	arn:${Partition}:devicefarm:${Region}:${Account}:test:${ResourceId}	
upload	arn:${Partition}:devicefarm:${Region}:${Account}:upload:${ResourceId}	
artifact	arn:${Partition}:devicefarm:${Region}:${Account}:artifact:${ResourceId}	
sample	arn:${Partition}:devicefarm:${Region}:${Account}:sample:${ResourceId}	
networkprofile	arn:${Partition}:devicefarm:${Region}:${Account}:networkprofile:${ResourceId}	aws:ResourceTag/${TagKey}
deviceinstance	arn:${Partition}:devicefarm:${Region}::deviceinstance:${ResourceId}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:devicefarm:${Region}:${Account}:session:${ResourceId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
devicepool	arn:${Partition}:devicefarm:${Region}:${Account}:devicepool:${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:devicefarm:${Region}::device:${ResourceId}	aws:ResourceTag/${TagKey}
instanceprofile	arn:${Partition}:devicefarm:${Region}:${Account}:instanceprofile:${ResourceId}	aws:ResourceTag/${TagKey}
vpceconfiguration	arn:${Partition}:devicefarm:${Region}:${Account}:vpceconfiguration:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-project	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-project:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-session	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-session:${ResourceId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Device Farm

AWS Device Farm define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función del conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado con el recurso.	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de etiquetas obligatorias en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición de Amazon DevOps Guru

Amazon DevOps Guru (prefijo de servicio:`devops-guru`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon DevOps Guru
- Tipos de recursos definidos por Amazon DevOps Guru
- Claves de condición de Amazon DevOps Guru

Acciones definidas por Amazon DevOps Guru

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddNotificationChannel	Otorga permiso para añadir un canal de notificaciones a Guru DevOps	Escritura	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
DeleteInsight	Otorga permiso para eliminar información específica en su cuenta	Escritura			
DescribeAccountHealth	Otorga permiso para ver el estado de las operaciones de su Cuenta de AWS	Lectura			
DescribeAccountOverview	Otorga permiso para ver el estado de las operaciones dentro de un intervalo de tiempo en su Cuenta de AWS	Lectura			
DescribeAnomaly	Concede permiso para enumerar los detalles de una anomalía específica	Lectura			
DescribeEventSourcesConfig	Otorga permiso a DevOps Guru para recuperar detalles sobre las fuentes de los eventos	Lectura			
DescribeFeedback	Concede permiso para ver los detalles de los comentarios de una información específica	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInsight	Concede permiso para enumerar los detalles de una información específica	Lectura			
DescribeOrganizationHealth	Concede permiso para ver el estado de las operaciones de su organización	Lectura			
DescribeOrganizationOverview	Concede permiso para ver el estado de las operaciones de su organización dentro de un rango de tiempo	Lectura			
DescribeOrganizationResourceCollectionHealth	Otorga permiso para ver el estado de las operaciones de cada AWS CloudFormation pila, AWS servicio o cuenta especificados en DevOps Guru en su organización	Lectura			
DescribeResourceCollectionHealth	Otorga permiso para ver el estado de las operaciones de cada AWS CloudFormation pila especificada en DevOps Guru	Lectura			
DescribeServiceIntegration	Otorga permiso para ver el estado de integración de los servicios que se pueden integrar con DevOps Guru	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCostEstimation	Concede permiso para enumerar estimaciones de costos de recursos de servicio	Lectura			
GetResourceCollection	Otorga permiso para enumerar las AWS CloudFormation pilas que DevOps Guru está configurado para usar	Lectura			
ListAnomaliesForInsight	Concede permiso para enumerar las anomalías de una información determinada de su cuenta	Enumeración		devops-guru:ServiceNames	
ListAnomalousLogGroups	Otorga permiso para enumerar las anomalías de registro de una información determinada de su cuenta.	Enumeración			
ListEvents	Otorga permiso para enumerar los eventos de recursos que son evaluados por Guru DevOps	Enumeración			
ListInsights	Concede permiso para enumerar las informaciones de su cuenta	Enumeración			
ListMonitoredResources	Otorga permiso para incluir en su cuenta los recursos monitoreados por DevOps Guru	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNotificationChannels	Otorga permiso para incluir en su cuenta los canales de notificación configurados para DevOps Guru	Enumeración			
ListOrganizationInsights	Concede permiso para enumerar las informaciones de su organización	Enumeración			
ListRecommendations	Concede permiso para enumerar las recomendaciones de una información específica	Enumeración			
PutFeedback	Otorga permiso para enviar comentarios a DevOps Guru	Escritura			
RemoveNotificationChannel	Otorga permiso para eliminar un canal de notificaciones de DevOps Guru	Escritura	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	Concede permiso para buscar información en su cuenta	Enumeración		devops-guru:ServiceNames	
SearchOrganizationInsights	Concede permiso para buscar información en su organización	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCostEstimation	Concede permiso para iniciar la creación de una estimación del costo mensual	Lectura			
UpdateEventSourcesConfig	Otorga permiso para actualizar la fuente de un evento de DevOps Guru	Escritura			
UpdateResourceCollection	Otorga permiso para actualizar la lista de AWS CloudFormation pilas que se utilizan para especificar qué AWS recursos de tu cuenta analiza Guru DevOps	Escritura			
UpdateServiceIntegration	Otorga permiso para activar o desactivar un servicio que se integra con DevOps Guru	Escritura			

Tipos de recursos definidos por Amazon DevOps Guru

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	

Claves de condición de Amazon DevOps Guru

Amazon DevOps Guru define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
devops-guru:ServiceNames	Filtra el acceso por API para restringir el acceso a determinados nombres AWS de servicios	ArrayOfString

Acciones, recursos y claves de condición de las herramientas AWS Diagnostic

AWS Las herramientas de diagnóstico (prefijo de servicio:`ts`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las herramientas AWS Diagnostic
- Tipos de recursos definidos por herramientas AWS Diagnostic
- Claves de condición para las herramientas AWS Diagnostic

Acciones definidas por las herramientas AWS Diagnostic

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetExecution	Otorga permiso para obtener detalles sobre la ejecución específica en las herramientas de AWS diagnóstico	Lectura	execution*		
GetExecutionOutput	Otorga permiso para obtener detalles sobre un resultado de ejecución específico en las herramientas AWS de diagnóstico	Lectura	execution*		
GetTool	Otorga permiso para obtener detalles sobre una herramienta específica dentro de las herramientas AWS de diagnóstico	Lectura	tool*		
ListExecutions	Otorga permiso para enumerar todas las ejecuciones disponibles en las	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	herramientas AWS de diagnóstico				
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso AWS de herramientas de diagnóstico	Lectura	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTools	Otorga permiso para enumerar todas las herramientas disponibles en las herramientas AWS de diagnóstico	Enumeración			
StartExecution	Otorga permiso para iniciar un flujo de trabajo de ejecución de una herramienta específica dentro de las herramientas AWS de diagnóstico	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
TagResource	Otorga permiso para etiquetar un recurso AWS de herramientas de diagnóstico	Etiquetado	execution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para desetiquetar un recurso AWS de herramientas de diagnóstico	Etiquetado	execution*		
				aws:TagKeys	

Tipos de recursos definidos por herramientas AWS Diagnostic

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
execution	`arn:${Partition}:ts::${Account}:execution/${UserId}/${ToolId}/${ExecutionId}`	aws:ResourceTag/${TagKey}
tool	`arn:${Partition}:ts::aws:tool/${ToolId}`	

Claves de condición para las herramientas AWS Diagnostic

AWS Las herramientas de diagnóstico definen las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Direct Connect

AWS Direct Connect (prefijo de servicio:`directconnect`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Direct Connect
- Tipos de recursos definidos por AWS Direct Connect
- Claves de condición para AWS Direct Connect

Acciones definidas por AWS Direct Connect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptDirectConnectGatewayAssociationProposal	Otorga permisos para aceptar una solicitud de propuesta de asociar una puerta de enlace privada virtual a una puerta de enlace de Direct Connect.	Escritura	dx-gateway*		
AllocateConnectionOnInterconnect	Otorga permisos para crear una conexión alojada en una interconexión.	Escritura	dxcon*		
AllocateHostedConnection	Otorga permiso para crear una nueva conexión alojada entre la red de un socio de AWS Direct Connect y una ubicación específica de AWS Direct Connect	Escritura	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	Otorga permisos para aprovisionar una interfaz virtual privada para que sea propiedad de otro cliente.	Escritura	dxcon		
			dxlag		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePublicVirtualInterface	Otorga permisos para aprovisionar una interfaz virtual pública para que sea propiedad de otro cliente.	Escritura	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocateTransitVirtualInterface	Otorga permisos para aprovisionar una interfaz virtual de tránsito para que sea propiedad de otro cliente.	Escritura	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	Otorga permisos para asociar una conexión con un LAG.	Escritura	dxcon*		
			dxlag*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateHostedConnection	Otorga permisos para asociar una conexión alojada y sus interfaces virtuales con una interconexión o un grupo de agregación de enlaces (LAG).	Escritura	dxcon*		
			dxcon		
			dxlag		
AssociateMacSecKey	Otorga permiso para asociar un par de nombre de clave de conexión (CKN) y clave de asociación de conectividad (CAK) MAC a una conexión dedicada de AWS Direct Connect MACsec	Escritura	dxcon		
			dxlag		
AssociateVirtualInterface	Otorga permisos para asociar una interfaz virtual con una conexión o un grupo de agregación de enlaces (LAG) determinados.	Escritura	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	Otorga permisos para confirmar la creación de una conexión alojada en una interconexión.	Escritura	dxcon*		
ConfirmCustomerAgreement	Otorga permisos para confirmar los términos del acuerdo al crear la conexión o el grupo de agregación de enlaces (LAG).	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConfirmPrivateVirtualInterface	Otorga permisos para agregar la propiedad de una interfaz virtual privada creada por otro cliente.	Escritura	dxvif*		
ConfirmPublicVirtualInterface	Otorga permisos para aceptar la propiedad de una interfaz virtual pública creada por otro cliente.	Escritura	dxvif*		
ConfirmTransitVirtualInterface	Otorga permisos para aceptar la propiedad de una interfaz virtual de tránsito creada por otro cliente.	Escritura	dxvif*		
CreateBGPPeer	Otorga permisos para crear un BGP de mismo nivel en la interfaz virtual especificada.	Escritura	dxvif*		
CreateConnection	Otorga permiso para crear una nueva conexión entre la red del cliente y una ubicación específica de AWS Direct Connect	Escritura	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDirectConnectGateway	Otorga permisos para crear una puerta de enlace de Direct Connect, que es un objeto intermedio que le permite conectar un conjunto de interfaces virtuales y puertas de enlace privadas virtuales.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAssociation	Otorga permisos para crear una asociación entre una gateway de Direct Connect y una puerta de enlace privada virtual.	Escritura	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	Otorga permisos para crear una propuesta para asociar la puerta de enlace privada virtual especificada con la puerta de enlace de Direct Connect especificada.	Escritura	dx-gateway*		
CreateInterconnect	Otorga permiso para crear una nueva interconexión entre la red de un socio de AWS Direct Connect y una ubicación específica de AWS Direct Connect	Escritura	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLag	Otorga permiso para crear un grupo de agregación de enlaces (LAG) con el número especificado de conexiones físicas agrupadas entre la red del cliente y una ubicación específica de AWS Direct Connect	Escritura	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateVirtualInterface	Otorga permisos para crear una interfaz privada virtual.	Escritura	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	Otorga permisos para crear una nueva interfaz virtual pública.	Escritura	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	Otorga permisos para crear una nueva interfaz virtual de tránsito.	Escritura	dxcon		
			dxlag		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBGPPeer	Otorga permisos para eliminar el BGP de mismo nivel especificado en la interfaz virtual especificada con la dirección y ASN del cliente especificados.	Escritura	dxvif*		
DeleteConnection	Otorga permisos para eliminar una conexión.	Escritura	dxcon*		
DeleteDirectConnectGateway	Otorga permisos para eliminar la puerta de enlace Direct Connect especificada.	Escritura	dx-gateway*		
DeleteDirectConnectGatewayAssociation	Otorga permisos para eliminar la asociación entre la puerta de enlace de Direct Connect especificada y la puerta de enlace privada virtual.	Escritura	dx-gateway*		
DeleteDirectConnectGatewayAssociationProposal	Otorga permisos para eliminar la solicitud de propuesta de asociación entre la puerta de enlace de Direct Connect especificada y la puerta de enlace privada virtual.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteInterconnect	Otorga permisos para eliminar la interconexión especificada.	Escritura	dxcon*		
DeleteLag	Otorga permisos para eliminar el grupo de agregación de enlaces (LAG).	Escritura	dxlag*		
DeleteVirtualInterface	Otorga permisos para eliminar una interfaz virtual.	Escritura	dxvif*		
DescribeConnectionLoa	Otorga permisos para describir el documento LOA-CFA para una conexión.	Lectura	dxcon*		
DescribeConnections	Otorga permisos para describir todas las conexiones en esta región.	Lectura	dxcon		
DescribeConnectionsOnInterconnect	Otorga permisos para describir una lista de las conexiones que se han aprovisionado en la interconexión determinada.	Lectura	dxcon*		
DescribeCustomerMetadata	Otorga permiso para ver una lista de los acuerdos con los clientes, junto con su estado de firma y si el cliente es un NNIPartner socio, NNIPartner V2 o no	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDirectConnectGatewayAssociationProposals	Otorga permisos para describir una o varias propuestas de asociación para la conexión entre una puerta de enlace privada virtual y una puerta de enlace de Direct Connect.	Lectura	dx-gateway		
DescribeDirectConnectGatewayAssociations	Otorga permisos para describir todas las asociaciones entre las puertas de enlace de Direct Connect y las puertas de enlace privadas virtuales.	Lectura	dx-gateway		
DescribeDirectConnectGatewayAttachments	Otorga permisos para describir las vinculaciones entre las puertas de enlace de Direct Connect y las interfaces virtuales.	Lectura	dx-gateway		
DescribeDirectConnectGateways	Otorga permisos para describir todas las puertas de enlace de Direct Connect o solo las puertas de enlace de Direct Connect especificadas.	Lectura	dx-gateway		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeHostedConnections	Otorga permisos para describir las conexiones alojadas que se han aprovisionado en la interconexión o el grupo de agregación de enlaces (LAG) especificados.	Lectura	dxcon dxlag		
DescribeInterconnectLoa	Otorga permisos para describir el documento LOA-CFA para una interconexión.	Lectura	dxcon*		
DescribeInterconnects	Otorga permiso para describir una lista de interconexiones propiedad de Cuenta de AWS	Lectura	dxcon		
DescribeLags	Otorga permisos para describir todos los grupos de agregación de enlaces (LAG) o el LAG especificado.	Lectura	dxlag		
DescribeLoa	Otorga permisos para describir el documento LOA-CFA para una conexión, interconexión o grupo de agregación de enlaces (LAG).	Lectura	dxcon dxlag		
DescribeLocations	Otorga permiso para describir la lista de ubicaciones de AWS Direct Connect en la AWS región actual	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRouterConfiguration	Otorga permisos para describir detalles sobre el enrutador de una interfaz virtual.	Lectura	dxvif*		
DescribeTags	Otorga permiso para describir las etiquetas asociadas a los recursos de AWS Direct Connect especificados	Lectura	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
DescribeVirtualGateways	Otorga permiso para describir una lista de puertas de enlace privadas virtuales propiedad del Cuenta de AWS	Lectura			
DescribeVirtualInterfaces	Otorga permiso para describir todas las interfaces virtuales de un Cuenta de AWS	Lectura	dxcon		
			dxlag		
			dxvif		
DisassociateConnectionFromLag	Otorga permisos para desasociar una conexión de un grupo de agregación de enlaces (LAG).	Escritura	dxcon*		
			dxlag*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateMacSecKey	Otorga permiso para eliminar la asociación entre una clave de seguridad MAC Security (MACsec) y una conexión dedicada de AWS Direct Connect	Escritura	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	Otorga permisos para enumerar el historial de pruebas de conmutación por error de la interfaz virtual.	Enumeración	dxvif*		
StartBgpFailoverTest	Otorga permisos para iniciar la prueba de conmutación por error de la interfaz virtual, que verifica si la configuración cumple los requisitos de resistencia asignando el estado DOWN a la sesión de intercambio de tráfico (peering) BGP. A continuación, puede enviar tráfico para comprobar que no hay interrupciones.	Escritura	dxvif*		
StopBgpFailoverTest	Otorga permisos para detener la prueba de conmutación por error de interfaz virtual.	Escritura	dxvif*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar las etiquetas especificadas al recurso de AWS Direct Connect especificado. Cada recurso puede tener un máximo de 50 etiquetas.	Etiquetado	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una o más etiquetas del recurso AWS Direct Connect especificado	Etiquetado	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnection	Concede permiso para actualizar la configuración de conexión dedicada de AWS Direct Connect. Puede actualizar los siguientes parámetros de una conexión: el nombre de la conexión o el modo de cifrado MAC Security (MACsec) de la conexión	Escritura	dxcon*		
UpdateDirectConnectGateway	Otorga permisos para actualizar el nombre de una puerta de enlace de Direct Connect.	Escritura	dx-gateway*		
UpdateDirectConnectGatewayAssociation	Otorga permisos para actualizar los atributos especificados de la asociación de la puerta de enlace de Direct Connect.	Escritura			
UpdateLag	Otorga permisos para actualizar los atributos del grupo de agregación de enlaces (LAG) especificado.	Escritura	dxlag*		
UpdateVirtualInterfaceAttributes	Otorga permisos para actualizar los atributos especificados de la interfaz privada virtual especificada.	Escritura	dxvif*		

Tipos de recursos definidos por AWS Direct Connect

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey}
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`	aws:ResourceTag/${TagKey}
dxvif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`	aws:ResourceTag/${TagKey}
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Direct Connect

AWS Direct Connect define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante acciones en función de pares de clave-valor asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante acciones en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Directory Service

AWS Directory Service (prefijo de servicio:`ds`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Directory Service
- Tipos de recursos definidos por AWS Directory Service
- Claves de condición para AWS Directory Service

Acciones definidas por AWS Directory Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptSharedDirectory	Concede permiso para aceptar una solicitud de directorio compartido enviada desde la cuenta del propietario del directorio	Write	directory*		
AccessDSData [solo permiso]	Concede permiso para acceder a los datos del directorio mediante la API de Directory Service Data	Administración de permisos	directory*		
AddIpRoutes	Concede permiso para agregar un bloque de direcciones de CIDR para dirigir correctamente el tráfico hacia y desde su Microsoft AD en Amazon Web Services	Escritura	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups
AddRegion	Concede permiso para agregar dos controladores de dominio en la región establecida para el directorio especificado	Escritura	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecur

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
AddTagsToResource	Concede permiso para agregar o sobrescribir una o varias etiquetas para el directorio especificado de Amazon Directory Services	Etiquetado	directory*		ec2:CreateTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
AuthorizeApplication [solo permiso]	Otorga permiso para autorizar una aplicación para su directorio AWS	Escritura	directory*		
CancelSchemaExtension	Concede permiso para cancelar una extensión de esquema en curso a un directorio de Microsoft AD	Escritura	directory*		
CheckAlias [solo permiso]	Concede permiso para verificar que el alias esté disponible para su uso	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConnectDirectory	Concede permiso para crear un AD Connector para conectarse a un directorio en las instalaciones	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAlias	Concede permiso para crear un alias para un directorio y asigna el alias al directorio	Escritura	directory*		
CreateComputer	Concede permiso para crear una cuenta de computadora en el directorio especificado y une la computadora al directorio	Escritura	directory*		
CreateConditionalForwarder	Otorga permiso para crear un reenviador condicional asociado a su directorio AWS	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDirectory	Concede permiso para crear un directorio Simple AD	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIdentityPoolDirectory [solo permiso]	Otorga permiso para crear un IdentityPool directorio en la nube AWS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogSubscription	Otorga permiso para crear una suscripción para reenviar los registros de seguridad del controlador de dominio de Directory Service en tiempo real al grupo de CloudWatch registros especificado en su Cuenta de AWS	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMicrosoftAD	Otorga permiso para crear un Microsoft AD en la AWS nube	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSnapshot	Otorga permiso para crear una instantánea de un directorio de Simple AD o Microsoft AD en la AWS nube	Escritura	directory*		
CreateTrust	Otorga permiso para iniciar la creación de la AWS parte de una relación de confianza entre un Microsoft AD en la AWS nube y un dominio externo	Escritura	directory*		
DeleteConditionalForwarder	Otorga permiso para eliminar un reenviador condicional que se haya configurado para su directorio AWS	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDirectory	Concede permiso para eliminar un AWS directorio de Directory Service	Escritura	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	Concede permiso para eliminar el registro de la suscripción especificado	Escritura	directory*		
DeleteSnapshot	Concede permiso para eliminar una instantánea de directorio	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTrust	Otorga permiso para eliminar una relación de confianza existente entre su Microsoft AD en la AWS nube y un dominio externo	Escritura	directory*		
DeregisterCertificate	Concede permiso para eliminar del sistema el certificado que fue registrado para una conexión LDAP segura	Escritura	directory*		
DeregisterEventTopic	Concede permiso para quitar el directorio especificado como publicador en el tema de SNS especificado	Escritura	directory*		
DescribeCertificate	Concede permiso para mostrar información sobre el certificado registrado para una conexión LDAP segura	Lectura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeClientAuthenticationSettings	Concede permiso para recuperar información sobre el tipo de autenticación de cliente para el directorio especificado, si se especifica el tipo. Si no se especifica ningún tipo, se recupera información sobre todos los tipos de autenticación de clientes que se admiten para el directorio especificado. Actualmente, solo SmartCard es compatible	Lectura	directory*		
DescribeConditionalForwarders	Concede permiso para obtener información acerca de los reenviadores condicionales para esta cuenta	Lectura	directory*		
DescribeDirectories	Concede permiso para obtener información acerca de los directorios que pertenecen a esta cuenta	Enumeración			
DescribeDirectoryDataAccess	Concede permiso para describir el estado de la API de Directory Service Data para el directorio especificado	Lectura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDomainControllers	Concede permiso para proporcionar información acerca de los controladores de dominio de su directorio	Lectura	directory*		
DescribeEventTopics	Concede permiso para obtener información acerca de qué temas de SNS reciben mensajes de estado desde el directorio especificado	Lectura	directory*		
DescribeLDAPSSettings	Concede permiso para escribir el estado de la seguridad de LDAP para el directorio especificado	Lectura	directory*		
DescribeRegions	Concede permiso para proporcionar información acerca de las regiones configuradas para la replicación de varias regiones	Lectura	directory*		
DescribeSettings	Concede permiso para recuperar información sobre los ajustes configurables para el directorio especificado.	Lectura	directory*		
DescribeSharedDirectories	Concede permiso para devolver los directorios compartidos de su cuenta	Lectura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSnapshots	Concede permiso para obtener información acerca de las instantáneas de directorios que pertenecen a esta cuenta	Lectura			
DescribeTrusts	Concede permiso para obtener información acerca de las relaciones de confianza de esta cuenta	Lectura			
DescribeUpdateDirectory	Concede permiso para describir las actualizaciones de un directorio correspondientes a un determinado tipo de actualización	Lectura	directory*		
DisableClientAuthentication	Concede permiso para desactivar los métodos alternativos de autenticación de clientes para el directorio especificado	Escritura	directory*		
DisableDirectoryDataAccess	Concede permiso para desactivar la API de Directory Service Data para el directorio especificado	Escritura	directory*		
DisableLDAPS	Concede permiso para desactivar las llamadas seguras LDAP para el directorio especificado	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableRadius	Concede permiso para desactivar la autenticación multifactor (MFA) con el servidor Remote Authentication Dial In User Service (RADIUS) para un directorio de AD Connector	Escritura	directory*		
DisableRoleAccess [solo permiso]	Otorga permiso para deshabilitar el AWS Management Console acceso a la identidad en su AWS directorio	Escritura	directory*		
DisableSso	Concede permiso para desactivar un ingreso de única vez para un directorio	Escritura	directory*		
EnableClientAuthentication	Concede permiso para habilitar métodos alternativos de autenticación de clientes para el directorio especificado	Escritura	directory*		
EnableDirectoryDataAccess	Concede permiso para habilitar la API de Directory Service Data para el directorio especificado	Escritura	directory*		
EnableLDAPS	Concede permiso para activar el control para que el directorio específico utilice llamadas seguras LDAP	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableRadius	Concede permiso para habilitar la autenticación multifactor (MFA) con el servidor Remote Authentication Dial In User Service (RADIUS) para un directorio de AD Connector	Escritura	directory*		
EnableRoleAccess [solo permiso]	Otorga permiso para permitir el AWS Management Console acceso a la identidad en su AWS Directorio	Escritura	directory*		iam:PassRole
EnableSso	Concede permiso para habilitar el inicio de sesión único para un directorio	Escritura	directory*		
GetAuthorizedApplicationDetails [solo permiso]	Concede permiso para recuperar los detalles de las aplicaciones autorizadas de un directorio	Lectura	directory*		
GetDirectoryLimits	Concede permiso para obtener información acerca del límite de directorios para la región actual	Lectura			
GetSnapshotLimits	Concede permiso para obtener los límites de la instantánea manual para un directorio	Lectura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAuthorizedApplications [solo permiso]	Otorga permiso para obtener las AWS aplicaciones autorizadas para un directorio	Lectura	directory*		
ListCertificates	Concede permiso para enumerar todos los certificados registrados para una conexión LDAP segura, para el directorio especificado	Enumeración	directory*		
ListIpRoutes	Concede permiso para enumerar los bloques de direcciones que ha agregado a un directorio	Lectura	directory*		
ListLogSubscriptions	Otorga permiso para enumerar las suscripciones de registro activas para Cuenta de AWS	Lectura			
ListSchemaExtensions	Concede permiso para enumerar todas las extensiones de esquema que se aplican a un directorio de Microsoft AD	Enumeración	directory*		
ListTagsForResource	Concede permiso para enumerar todas las etiquetas de un directorio de Amazon Directory Services	Lectura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterCertificate	Concede permiso para registrar un certificado para una conexión LDAP segura	Escritura	directory*		
RegisterEventTopic	Concede permiso para asociar un directorio a un tema de SNS	Escritura	directory*		sns:GetTopicAttributes
RejectSharedDirectory	Concede permiso para reflejar una solicitud de directorio compartido que se envió desde la cuenta del propietario del directorio	Escritura	directory*		
RemoveIpRoutes	Concede permiso para eliminar bloques de direcciones IP de un directorio	Escritura	directory*		
RemoveRegion	Concede permiso para detener toda la replicación y elimina los controladores de dominio de la región especificada. No puede eliminar la región principal con esta operación	Escritura	directory*		
RemoveTagsFromResource	Concede permiso para eliminar las etiquetas de un directorio de Amazon Directory Services	Etiquetado	directory*		ec2:DeleteTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetUserPassword	Otorga permiso para restablecer la contraseña de cualquier usuario del directorio Microsoft AD AWS administrado o Simple AD	Escritura	directory*		
RestoreFromSnapshot	Concede permiso para restaurar un directorio usando una instantánea de directorio existente	Escritura	directory*		
ShareDirectory	Otorga permiso para compartir un directorio específico de su Cuenta de AWS (propietario del directorio) con otro Cuenta de AWS (consumidor del directorio). Con esta operación, puede utilizar su directorio desde cualquier Cuenta de AWS Amazon VPC dentro de un Región de AWS	Escritura	directory*		
StartSchemaExtension	Concede permiso para aplicar una extensión de esquema a un directorio de Microsoft AD	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UnauthorizeApplication [solo permiso]	Otorga permiso para desautorizar una aplicación de su directorio AWS	Escritura	directory*		
UnshareDirectory	Concede permiso para detener el uso compartido de directorios entre el propietario del directorio y las cuentas del consumidor	Escritura	directory*		
UpdateAuthorizedApplication [solo permiso]	Otorga permiso para actualizar una aplicación autorizada para su Directorio AWS	Escritura	directory*		
UpdateConditionalForwarder	Otorga permiso para actualizar un reenviador condicional que se haya configurado para su directorio AWS	Escritura	directory*		
UpdateDirectory [solo permiso]	Concede permiso para actualizar las configuraciones, tales como credenciales de la cuenta de servicio o direcciones IP del servidor DNS, para el directorio especificado	Escritura	directory*		
UpdateDirectorySetup	Concede permiso para actualizar el directorio con un determinado tipo de actualización	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateNumberOfDomainControllers	Concede permiso para agregar o quitar controladores de dominio en el directorio o hacia el directorio. En función de la diferencia entre el valor actual y el valor nuevo (proporcionada a través de esta llamada a la API), los controladores de dominio se agregarán o eliminarán. Esta operación puede tardar hasta 45 minutos para que cualquier controlador de dominio nuevo pase a estar totalmente activo una vez que el número de controladores de dominio solicitados se actualice. Durante este tiempo, no puede realizar ninguna otra solicitud de actualización	Escritura	directory*		
UpdateRadius	Concede permiso para actualizar la información del servidor Remote Authentication Dial In User Service (RADIUS) para un directorio de AD Connector	Escritura	directory*		
UpdateSettings	Concede permiso para actualizar la configuración del directorio especificado.	Escritura	directory*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTrust	Otorga permiso para actualizar la confianza que se ha establecido entre el directorio AWS administrado de Microsoft AD y un Active Directory local	Escritura	directory*		
VerifyTrust	Otorga permiso para verificar una relación de confianza entre su Microsoft AD en la AWS nube y un dominio externo	Lectura	directory*		

Tipos de recursos definidos por AWS Directory Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Directory Service

AWS Directory Service define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el valor de la solicitud a AWS DS	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por parte del recurso AWS de DS sobre el que se está actuando	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Directory Service Data

AWS Directory Service Data (prefijo de servicio:`ds-data`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Directory Service Data
- Tipos de recursos definidos por AWS Directory Service Data
- Claves de condición para AWS Directory Service Data

Acciones definidas por AWS Directory Service Data

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddGroupMember	Concede permiso para agregar un miembro a un grupo en un directorio	Escritura	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
CreateGroup	Concede permiso para crear un grupo en un directorio	Escritura	directory*		ds:AccessDSData

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
CreateUser	Concede permiso para crear un usuario en un directorio	Escritura	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteGroup	Concede permiso para eliminar un grupo en un directorio	Escritura	directory*		ds:AccessDSData

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteUser	Concede permiso para eliminar un usuario en un directorio	Escritura	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeGroup	Concede permiso para describir un grupo en un directorio	Lectura	directory*		ds:AccessDSData

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeUser	Concede permiso para describir un usuario en un directorio	Lectura	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DisableUser	Concede permiso para desactivar un usuario en un directorio	Escritura	directory*		ds:AccessDSData

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
ListGroupMembers	Concede permiso para enumerar miembros de un grupo en un directorio	Enumeración	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListGroups	Concede permiso para enumerar grupos en un directorio	Enumeración	directory*		ds:AccessDSData
				ds-data:Realm	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGroupsForMember	Concede permiso para enumerar los grupos a los que pertenece un miembro en un directorio	Enumeración	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListUsers	Concede permiso para enumerar usuarios en un directorio	Enumeración	directory*		ds:AccessDSData
				ds-data:Realm	
RemoveGroupMember	Concede permiso para eliminar a un miembro de un grupo en un directorio	Escritura	directory*		ds:AccessDSData

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
SearchGroups	Concede permiso para buscar grupos en un directorio	Lectura	directory*		ds-data:DescribeGroup ds:AccessDSData
				ds-data:Realm	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchUsers	Concede permiso para buscar usuarios en un directorio	Lectura	directory*		ds-data:DescribeUser ds:AccessDSData
				ds-data:Realm	
UpdateGroup	Concede permiso para actualizar un grupo en un directorio	Escritura	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
UpdateUser	Concede permiso para actualizar un usuario en un directorio	Escritura	directory*		ds:AccessDSData

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

Tipos de recursos definidos por AWS Directory Service Data

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Directory Service Data

AWS Directory Service Data define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por parte del recurso AWS de DS sobre el que se está actuando	Cadena
ds-data:Identifier	Filtra el acceso por el tipo de identificador proporcionado en la solicitud (es decir, nombre de cuenta SAM).	Cadena
ds-data:MemberName	Filtra el acceso por el nombre de la cuenta SAM del directorio incluido en la MemberName entrada de la solicitud	Cadena
ds-data:MemberRealm	Filtra el acceso por el nombre de dominio del directorio incluido en la MemberRealm entrada de la solicitud	Cadena
ds-data:Realm	Filtra el acceso por el nombre del ámbito del directorio de la solicitud	Cadena
ds-data:SAMAccountName	Filtra el acceso por el nombre de la cuenta SAM del directorio incluido en la entrada de SAMAccount nombre de la solicitud	Cadena

Acciones, recursos y claves de condición para Amazon DocumentDB Elastic Clusters

Amazon DocumentDB Elastic Clusters (prefijo de servicio: `docdb-elastic`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon DocumentDB Elastic Clusters
- Tipos de recursos definidos por Amazon DocumentDB Elastic Clusters
- Claves de condición de Amazon DocumentDB Elastic Clusters

Acciones definidas por Amazon DocumentDB Elastic Clusters

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApplyPendingMaintenanceAction	Otorga permiso para aplicar acciones de mantenimiento pendientes en el clúster Amazon DocDB-Elastic	Escritura	cluster*		
				aws:ResourceTag/${TagKey}	
CopyClusterSnapshot	Concede permiso para copiar una nueva instantánea de clúster de Amazon DocDB-Elastic	Escritura	cluster-snapshot*		docdb-elastic:CreateClusterSnapshot kms:CreateGrant kms:Decrypt

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					kms:DescribeKey kms:GenerateDataKey
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCluster	Otorga permiso para crear un nuevo clúster de Amazon DocDB Elastic	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateClusterSnapshot	Otorga permiso para crear una nueva instantánea de un clúster de Amazon DocDB Elastic	Escritura	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCluster	Otorga permiso para eliminar un clúster	Escritura	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteClusterSnapshot	Otorga permiso para eliminar una instantánea de un clúster	Escritura	cluster-snapshot*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetCluster	Otorga permiso para ver detalles sobre un clúster	Lectura	cluster*		
				aws:ResourceTag/${TagKey}	
GetClusterSnapshot	Otorga permiso para ver detalles sobre una instantánea de un clúster	Lectura	cluster-snapshot*		
				aws:ResourceTag/${TagKey}	
GetPendingMaintenanceAction	Otorga permiso para ver detalles sobre las acciones de mantenimiento pendientes en el clúster Amazon DocDB-Elastic	Lectura	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusterSnapshots	Otorga permiso para enumerar las instantáneas del clúster de su cuenta	Enumeración			
ListClusters	Otorga permiso para enumerar los clústeres de su cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPendingMaintenanceActions	Otorga permiso para enumerar detalles sobre las acciones de mantenimiento pendientes en cualquier clúster de Amazon DocDB-Elastic	Enumeración		aws:ResourceTag/${TagKey}	
ListTagsForResource	Otorga permiso para enumerar etiquetas para un recurso de DocumentDB Elastic	Enumeración	cluster		
			cluster-snapshot		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreClusterFromSnapshot	Otorga permiso para restaurar el clúster a partir de una instantánea del clúster de Amazon DocDB Elastic	Escritura	cluster*		docdb-elastic:CreateCluster ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeVpcs ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:GetSecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
StartCluster	Concede permiso para iniciar un clúster de Amazon DocDB-Elastic detenido	Escritura	cluster*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopCluster	Concede permiso para detener un clúster de Amazon DocDB-Elastic existente	Escritura	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Otorga permiso para etiquetar un recurso de DocumentDB Elastic	Etiquetado	cluster		
			cluster-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para quitar la etiqueta de un recurso de DocumentDB Elastic	Etiquetado	cluster		
			cluster-snapshot		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCluster	Otorga permiso para modificar un clúster	Escritura	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:ModifyVpcEndpoint kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:Lis

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					tSecretVersionIds secretsmanager:ListSecrets
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon DocumentDB Elastic Clusters

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
cluster-snapshot	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon DocumentDB Elastic Clusters

Amazon DocumentDB Elastic Clusters define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante los pares clave-valor de la etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante los pares clave-valor de etiqueta adjuntados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante el conjunto de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para Amazon DynamoDB

Amazon DynamoDB (prefijo de servicio: `dynamodb`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon DynamoDB
- Tipos de recurso definidos por Amazon DynamoDB
- Claves de condición de Amazon DynamoDB

Acciones definidas por Amazon DynamoDB

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetItem	Otorga permisos para devolver los atributos de uno o varios elementos de una o varias tablas.	Lectura	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	Otorga permisos para colocar o eliminar varios elementos en una o varias tablas.	Escritura	table*		
				dynamodb:Attributes dynamodb:LeadingKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				dynamodb:ReturnConsumedCapacity	
ConditionCheckItem	Concede permiso a la ConditionCheckItem operación, comprueba la existencia de un conjunto de atributos para el elemento con la clave principal proporcionada	Lectura	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	Otorga permisos para crear una copia de seguridad de una tabla existente.	Escritura	table*		
CreateGlobalTable	Otorga permisos para crear una tabla global a partir de una tabla existente.	Escritura	global-table*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGlobalTableWitness [solo permiso]	Otorga permiso para añadir un testigo a una tabla global	Escritura	table*		
CreateTable	Concede permiso a la CreateTable operación y añade una tabla nueva a su cuenta	Escritura	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTableReplica [solo permiso]	Otorga permisos para agregar una nueva réplica de tabla.	Escritura	table*		
DeleteBackup	Otorga permisos para eliminar una copia de seguridad existente de una tabla.	Escritura	backup*		
DeleteGlobalTableWitness [solo permiso]	Otorga permiso para eliminar un testigo de una tabla global	Escritura	table*		
DeleteItem	Otorga permisos para eliminar un solo elemento de una tabla por clave principal.	Escritura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
DeleteResourcePolicy	Concede permiso para eliminar la política basada en recursos asociada al recurso	Administración de permisos	stream* table*		
DeleteTable	Otorga permiso a la DeleteTable operación que elimina una tabla y todos sus elementos	Escritura	table*		
DeleteTableReplica [solo permiso]	Otorga permisos para eliminar una réplica de tabla y todos sus elementos.	Escritura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBackup	Otorga permisos para describir una copia de seguridad existente de una tabla.	Lectura	backup*		
DescribeContinuousBackups	Otorga permisos para verificar el estado de la configuración de restauración de copia de seguridad en la tabla especificada.	Lectura	table*		
DescribeContributorInsights	Otorga permisos para describir el estado de Contributor Insights y los detalles relacionados de una tabla o un índice secundario global determinados.	Lectura	table* index		
DescribeEndpoints	Otorga permiso para devolver la información de punto de conexión regional	Lectura			
DescribeExport	Otorga permisos para describir una exportación existente de una tabla.	Lectura	export*		
DescribeGlobalTable	Otorga permisos para devolver información sobre la tabla global especificada.	Lectura	global-table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeGlobalTableSettings	Otorga permisos para devolver información de configuración sobre la tabla global especificada.	Lectura	global-table*		
DescribeImport	Concede permiso para describir una importación existente.	Lectura	import*		
DescribeKinesisStreamingDestination	Otorga permisos para describir el estado del streaming de Kinesis y los detalles relacionados de una tabla determinada.	Lectura	table*		
DescribeLimits	Otorga permiso para devolver los límites de capacidad aprovisionada actuales de una región, tanto para la región Cuenta de AWS en su conjunto como para cualquier tabla de DynamoDB que cree allí	Lectura			
DescribeReservedCapacity [solo permiso]	Otorga permisos para describir una o más de las capacidades reservadas adquiridas.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReservedCapacityOfferings [solo permiso]	Otorga permisos para describir las ofertas de capacidades reservadas que están disponibles para la compra.	Lectura			
DescribeStream	Otorga permisos para devolver información sobre una transmisión, incluido el estado actual de la transmisión, su nombre de recurso de Amazon (ARN), la composición de sus fragmentos y su tabla de DynamoDB correspondiente.	Lectura	stream*		
DescribeTable	Otorga permisos para devolver información acerca de las tareas exportadas.	Lectura	table*		
DescribeTableReplicaAutoScaling	Otorga permisos para describir la configuración de Auto Scaling en todas las réplicas de la tabla global.	Lectura	table*		
DescribeTimeToLive	Otorga permisos para proporcionar una descripción del estado de periodo de vida (TTL) en la tabla especificada.	Lectura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableKinesisStreamingDestination	Otorga permisos para otorgar permisos para detener la replicación de la tabla de DynamoDB en Kinesis Data Streams.	Escritura	table*		
EnableKinesisStreamingDestination	Otorga permisos para otorgar permisos para iniciar la replicación de los datos de la tabla en el flujo de datos de Kinesis especificado en una marca temporal elegida durante el flujo de trabajo de habilitación.	Escritura	table*		
ExportTableToPointInTime	Otorga permisos para iniciar una exportación de una tabla de DynamoDB a S3.	Escritura	table*		
GetAbacStatus [solo permiso]	Otorga permiso para ver el estado del control de acceso basado en atributos de la cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetItem	Otorga permiso a la GetItem operación que devuelve un conjunto de atributos para el elemento con la clave principal proporcionada	Lectura	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	Otorga permisos para recuperar los registros de transmisión de un fragmento determinado.	Lectura	stream*		
GetResourcePolicy	Concede permiso para ver una política basada en recursos para un recurso	Lectura	stream*		
			table*		
GetShardIterator	Otorga permisos para devolver un iterador de fragmentos.	Lectura	stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportTable	Concede permiso para iniciar una exportación desde S3 a una tabla de DynamoDB.	Escritura	table*		
ListBackups	Otorga permisos para enumerar las copias de seguridad asociadas a la cuenta y el punto de conexión.	Enumeración			
ListContributorInsights	Otorga permiso ContributorInsightsSummary para enumerar todas las tablas e índices secundarios globales asociados a la cuenta corriente y al punto final	Enumeración			
ListExports	Otorga permisos para enumerar las exportaciones asociadas a la cuenta y al punto de conexión.	Enumeración			
ListGlobalTables	Otorga permisos para enumerar todas las tablas globales que tienen una réplica en la región especificada.	Enumeración			
ListImports	Concede permiso para enumerar las importaciones asociadas a la cuenta y el punto de conexión.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStreams	Otorga permiso para devolver una matriz de flujos ARNs asociada a la cuenta corriente y al punto final	Lectura			
ListTables	Otorga permisos para devolver una matriz de los nombres de las tablas asociados con la cuenta y el punto de conexión actuales.	Enumeración			
ListTagsOfResource	Otorga permisos para enumerar todas las etiquetas de un recurso de Amazon DynamoDB.	Lectura	table*		
PartiQLDelete	Otorga permiso para eliminar un solo elemento de una tabla por clave principal	Write	table*	dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PartiQLInsert	Otorga permiso para crear un nuevo elemento, si no existe en la tabla un elemento con la misma clave principal	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	Otorga permiso para leer un conjunto de atributos de los elementos de una tabla o un índice	Read	table*		
			index		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PartiQLUpdate	Otorga permiso para editar los atributos de un elemento existente	Escritura	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PurchaseReservedCapacityOfferings [solo permiso]	Otorga permisos para comprar una capacidad reservada para su uso con su cuenta.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutItem	Otorga permisos para crear un nuevo elemento o sustituye un elemento antiguo por uno nuevo.	Escritura	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	Concede permiso para asociar una política basada en recursos al recurso	Administración de permisos	stream*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Query	Otorga permisos para utilizar la clave principal de una tabla o un índice secundario o para acceder directamente a elementos de esa tabla o índice.	Lectura	table*		
			index		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
RestoreTableFromAwsBackup [solo permiso]	Otorga permiso para crear una tabla nueva desde el punto de recuperación de AWS Backup	Escritura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreTableFromBackup	Otorga permisos para crear una nueva tabla a partir de una copia de seguridad existente.	Escritura	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreTableToPointInTime	Otorga permisos para restaurar una tabla a un punto en el tiempo.	Escritura	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Scan	Otorga permisos para devolver uno o varios elementos y atributos de elementos obteniendo acceso a todos los elementos de una tabla o un índice secundario.	Lectura	table*		
			index		
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob [solo permiso]	Otorga permiso para crear una copia de seguridad en AWS Backup con las funciones avanzadas habilitadas	Escritura	table*		
TagResource	Otorga permisos para asociar un conjunto de etiquetas con un recurso de Amazon DynamoDB.	Etiquetado	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permisos para eliminar la asociación de etiquetas de un recurso de Amazon DynamoDB.	Etiquetado	table*		
				aws:TagKeys	
UpdateAbacStatus [solo permiso]	Otorga permiso para actualizar el estado del control de acceso basado en atributos de la cuenta	Administración de permisos			
UpdateContinuousBackups	Otorga permiso para habilitar o desactivar copias de seguridad continuas.	Escritura	table*		
UpdateContributorInsights	Otorga permisos para actualizar el estado de Contributor Insights para una tabla o un índice secundario global específicos.	Escritura	table*		
			index		
UpdateGlobalTable	Otorga permisos para que el usuario agregue o elimine las réplicas de la tabla global especificada.	Escritura	global-table*		
			table*		
UpdateGlobalTableSettings	Otorga permisos para actualizar la configuración de un servicio global especificado.	Escritura	global-table*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGlobalTableVersion [solo permiso]	Otorga permiso para actualizar la versión de la tabla global especificado	Escritura	global-table*		
			table		
UpdateItem	Otorga permisos para editar los atributos de un elemento existente o agrega un nuevo elemento a la tabla, si no existe ya.	Escritura	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
UpdateKinesisStreamingDestination	Concede permiso para actualizar las configuraciones de replicación de datos para el flujo de datos de Kinesis especificado	Escritura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTable	Otorga permisos para modificar los ajustes de desempeño aprovisionado, índices secundarios globales o la configuración de DynamoDB Streams de una tabla determinada.	Escritura	table*		
UpdateTableReplicaAutoScaling	Otorga permisos para actualizar la configuración de Auto Scaling en la réplica de tabla.	Escritura	table*		
UpdateTimeToLive	Otorga permisos para habilitar o desactivar TTL para la tabla especificada.	Escritura	table*		

Tipos de recurso definidos por Amazon DynamoDB

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}`	
table	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}`	
export	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/export/${ExportName}`	
global-table	`arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}`	
import	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/import/${ImportName}`	

Claves de condición de Amazon DynamoDB

Amazon DynamoDB define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

> **Note**
>
> Para obtener información sobre cómo utilizar las claves de contexto para ajustar el acceso de DynamoDB mediante una política de IAM, consulte Uso de condiciones de políticas de IAM para control de acceso preciso en la Guía para desarrolladores de Amazon DynamoDB.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
dynamodb:Attributes	Filtra el acceso en función de los nombres de atributo (campo o columna) de la tabla	ArrayOfString
dynamodb:EnclosingOperation	Filtra el acceso bloqueando las APIs llamadas de Transactions y permitiendo las APIs llamadas que no son de Transaction y viceversa	Cadena
dynamodb:FullTableScan	Filtra el acceso bloqueando el escaneo completo de la tabla	Bool
dynamodb:LeadingKeys	Filtra el acceso en función de la clave de partición de la tabla	ArrayOfString
dynamodb:ReturnConsumedCapacity	Filtra el acceso por el ReturnConsumedCapacity parámetro de una solicitud. Contiene "TOTAL" o "NONE".	Cadena
dynamodb:ReturnValues	Filtra el acceso por el ReturnValues parámetro de la solicitud. Contiene una de las siguientes opciones:	Cadena

Claves de condición	Descripción	Tipo
	"ALL_OLD", "UPDATED_OLD","ALL_NEW","UP DATED_NEW" o "NONE".	
dynamodb: Select	Filtra el acceso en función del parámetro de Selección de una solicitud de Consulta o Escaneo	Cadena

Claves de condición, recursos y acciones para Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) (prefijo de servicio: `dax`) proporciona las siguientes claves de contexto de condiciones, acciones y recursos específicos de servicios para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon DynamoDB Accelerator (DAX)
- Tipos de recurso definidos por Amazon DynamoDB Accelerator (DAX)
- Claves de condición de Amazon DynamoDB Accelerator (DAX)

Acciones definidas por Amazon DynamoDB Accelerator (DAX)

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetItem	Otorga permisos para devolver los atributos de uno o varios elementos de una o varias tablas.	Lectura	application*		
BatchWriteItem	Otorga permisos para colocar o eliminar varios elementos en una o varias tablas.	Escritura	application*		
ConditionCheckItem	Otorga permiso a la ConditionCheckItem operación que comprueba la existencia de un conjunto de atributos para el elemento con la clave principal proporcionada	Lectura	application*		
CreateCluster	Concede permiso para crear un clúster DAX	Escritura	application*		dax:CreateParameterGroup dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole iam:PassRole
CreateParameterGroup	Concede permiso para crear un grupo de parámetros	Escritura			
CreateSubnetGroup	Otorga permiso para crear un grupo de subred	Escritura			
DecreaseReplicationFactor	Concede permiso para eliminar uno o varios nodos de un clúster de DAX	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCluster	Concede permiso para eliminar un clúster aprovisionado anteriormente DAX	Escritura	application*		
DeleteItem	Otorga permiso para eliminar un solo elemento de una tabla por clave principal	Escritura	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	Otorga permiso para eliminar el grupo de parámetros especificado	Escritura			
DeleteSubnetGroup	Otorga permiso para eliminar un grupo de subredes	Escritura			
DescribeClusters	Otorga permiso para devolver información acerca de los clústeres de DAX aprovisionados	Enumeración	application		
DescribeDefaultParameters	Otorga permiso para devolver información del parámetro del sistema predeterminado para DAX	Enumeración			
DescribeEvents	Otorga permisos para recuperar eventos relacionados con clústeres y grupos de seguridad de DAX	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeParameterGroups	Otorga permiso para devolver una lista de descripciones de grupos de parámetros	Enumeración			
DescribeParameters	Otorga permiso para devolver la lista de parámetros detallada para un grupo de parámetros concreto	Lectura			
DescribeSubnetGroups	Otorga permiso para devolver una lista de descripciones de grupos de subredes	Enumeración			
GetItem	Otorga permiso a la GetItem operación que devuelve un conjunto de atributos para el elemento con la clave principal dada	Lectura	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	Concede permiso para agregar uno o más nodos a un clúster de DAX.	Escritura	application*		
ListTags	Concede permiso para devolver una lista de todas las etiquetas de un clúster de DAX	Lectura	application*		
PutItem	Otorga permisos para crear un nuevo elemento o sustituye un elemento antiguo por uno nuevo.	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				dax:EnclosingOperation	
Query	Otorga permisos para utilizar la clave principal de una tabla o un índice secundario o para acceder directamente a elementos de esa tabla o índice.	Lectura	application*		
RebootNode	Concede permiso para reiniciar un solo nodo de un clúster DAX	Escritura	application*		
Scan	Otorga permisos para devolver uno o varios elementos y atributos de elementos obteniendo acceso a todos los elementos de una tabla o un índice secundario.	Lectura	application*		
TagResource	Otorga permiso para asociar un conjunto de etiquetas a un recurso DAX	Etiquetado	application*		
UntagResource	Otorga permisos para eliminar la asociación de etiquetas de un recurso DAX	Etiquetado	application*		
UpdateCluster	Otorga permiso con el fin de modificar la configuración para un clúster DAX	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateItem	Otorga permisos para editar los atributos de un elemento existente o agrega un nuevo elemento a la tabla, si no existe ya.	Escritura	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	Concede permiso para modificar los parámetros de un grupo de parámetros	Escritura			
UpdateSubnetGroup	Otorga permiso para modificar un grupo de subredes existente	Escritura			

Tipos de recurso definidos por Amazon DynamoDB Accelerator (DAX)

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Claves de condición de Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
dax:EnclosingOperation	Se utiliza para bloquear las APIs llamadas de Transactions y permitir las APIs llamadas que no son de Transaction y viceversa	Cadena

Claves de condición, recursos y acciones de Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling (prefijo de servicio:`autoscaling`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EC2 Auto Scaling
- Tipos de recursos definidos por Amazon EC2 Auto Scaling
- Claves de condición de Amazon EC2 Auto Scaling

Acciones definidas por Amazon EC2 Auto Scaling

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AttachInstances	Otorga permiso para adjuntar una o más EC2 instancias al grupo de Auto Scaling especificado	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	Concede permiso para adjuntar uno o varios grupos de destino al grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
AttachLoadBalancers	Concede permiso para adjuntar uno o varios equilibradores de carga al grupo de Auto Scaling especificado.	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Otorga permiso para adjuntar una o más fuentes de tráfico a un grupo de escalado automático	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
BatchDeleteScheduledAction	Concede permiso para eliminar la acciones programadas especificadas.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchPutScheduledUpdateGroupAction	Concede permiso para crear o actualizar varias acciones de escalado programadas para un grupo de Auto Scaling.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CancelInstanceRefresh	Concede permiso para cancelar una operación de actualización de instancia en curso	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CompleteLifecycleAction	Concede permiso para completar la acción de ciclo de vida para el token o la instancia especificados con el resultado especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAutoScalingGroup	Concede permiso para crear un grupo de Auto Scaling con el nombre y los atributos especificados.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBalancerNames	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfiguration	Concede permiso para crear una configuración de lanzamiento.	Write	launchConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:ImageId autoscaling:InstanceType autoscaling:SpotPrice autoscaling:MetadataHttpTokens autoscaling:MetadataHttpPutResponseHopLimit autoscaling:MetadataHttpEndpoint	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateOrUpdateTags	Concede permiso para crear o actualizar etiquetas para el grupo de Auto Scaling especificado	Etiquetado	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Concede permiso para eliminar el grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteLaunchConfiguration	Concede permiso para eliminar la configuración de lanzamiento especificada	Write	launchConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLifecycleHook	Concede permiso para eliminar el enlace de ciclo de vida especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotification Configuration	Concede permiso para eliminar la notificación especificada.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeletePolicy	Concede permiso para eliminar la política de Auto Scaling especificada.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteScheduledAction	Concede permiso para eliminar la acción programada especificadas.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	Concede permiso para eliminar las etiquetas especificadas.	Etiquetado	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteWarmPool	Concede permiso para eliminar el grupo de calentamiento asociado al grupo Auto Scaling	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	Otorga permiso para describir los límites de recursos actuales de Auto Scaling para su Cuenta de AWS	Enumeración			
DescribeAdjustmentTypes	Otorga permiso para describir los tipos de ajustes de política para su uso con PutScalingPolicy	Enumeración			
DescribeAutoScalingGroups	Concede permiso para describir uno o más grupos de Auto Scaling. Si no se proporciona una lista de nombres, la llamada describirá todos los grupos de Auto Scaling.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAutoScalingInstances	Concede permiso para describir una o varias instancias de Auto Scaling. Si no se proporciona una lista, la llamada describirá todas las instancias.	List			
DescribeAutoScalingNotificationTypes	Concede permiso para describir los tipos de notificación que son compatibles con Auto Scaling.	List			
DescribeInstanceRefreshes	Concede permiso para describir una o más actualizaciones de instancias para un grupo de Auto Scaling	List			
DescribeLaunchConfigurations	Concede permiso para describir una o varias conexiones de lanzamiento. Si omite la lista de nombres, la llamada describirá todas las configuraciones de lanzamiento.	List			
DescribeLifecycleHookTypes	Concede permiso para describir los tipos de enlaces de ciclo de vida disponibles.	List			
DescribeLifecycleHooks	Concede permiso para describir los enlaces de ciclo de vida del grupo de Auto Scaling especificado.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeLoadBalancerTargetGroups	Concede permiso para describir los grupos de destino del grupo de Auto Scaling especificado.	List			
DescribeLoadBalancers	Concede permiso para describir los equilibradores de carga del grupo de Auto Scaling especificado.	Enumeración			
DescribeMetricCollectionTypes	Otorga permiso para describir las CloudWatch métricas disponibles para Auto Scaling	Enumeración			
DescribeNotificationConfigurations	Concede permiso para describir las acciones de notificación asociadas al grupo de Auto Scaling especificado.	List			
DescribePolicies	Concede permiso para describir las políticas del grupo de Auto Scaling especificado.	List			
DescribeScalingActivities	Concede permiso para describir una o varias actividades de escalado para el grupo de Auto Scaling especificado.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeScalingProcessTypes	Otorga permiso para describir los tipos de procesos de escalado para usarlos con ResumeProcesses y SuspendProcesses	Enumeración			
DescribeScheduledActions	Concede permiso para describir las acciones programadas para su grupo de Auto Scaling que no se han ejecutado.	List			
DescribeTags	Concede permiso para describir las etiquetas especificadas.	Read			
DescribeTerminationPolicyTypes	Concede permiso para describir las políticas de terminación compatibles con Auto Scaling.	Enumeración			
DescribeTrafficSources	Concede permiso para describir los grupos de destino del grupo de Auto Scaling especificado.	Enumeración			
DescribeWarmPool	Concede permiso para describir el grupo de calentamiento asociado al grupo Auto Scaling	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetachInstances	Concede permiso para quitar una o varias instancias del grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	Concede permiso para desconectar uno o varios grupos de destino del grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
DetachLoadBalancers	Concede permiso para quitar uno o varios equilibradores de carga del grupo de Auto Scaling especificado.	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Otorga permiso para desconectar una o varias fuentes de tráfico de un grupo de escalado automático	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
DisableMetricsCollection	Concede permiso para desactivar el monitoreo de las métricas especificadas para el grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableMetricsCollection	Concede permiso para habilitar el monitoreo de las métricas especificadas para el grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	Concede permiso para mover las instancias especificadas al modo Standby (En espera).	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExecutePolicy	Concede permiso para ejecutar la política especificada.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExitStandby	Concede permiso para mover las instancias especificadas fuera del modo Standby (En espera).	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	Concede permiso para recuperar los datos de pronóstico de una política de escalado predictivo	Enumeración			
PutLifecycleHook	Concede permiso para crear o actualizar un enlace de ciclo de vida para el grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutNotificationConfiguration	Concede permiso para configurar un grupo de Auto Scaling para enviar notificaciones cuando se producen los eventos especificados.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Concede permiso para crear o actualizar una política para un grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScheduledUpdateGroupAction	Concede permiso para crear o actualizar una acción de escalado programada para un grupo de Auto Scaling.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	Concede permiso para crear o actualizar el grupo de calentamiento asociado con el grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RecordLifecycleActionHeartbeat	Concede permiso para registrar un latido para la acción de ciclo de vida asociada con el token o la instancia especificados.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResumeProcesses	Concede permiso para reanudar los procesos de Auto Scaling suspendidos especificados, o todos los procesos suspendidos, para el grupo de Auto Scaling especificado.	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	Otorga permiso para restaurar una operación de actualización de instancia en curso	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetDesiredCapacity	Concede permiso para establecer el tamaño del grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetInstanceHealth	Concede permiso para configurar el estado de la instancia especificada.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	Concede permiso para actualizar la configuración de protección de las instancias especificadas.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartInstanceRefresh	Concede permiso para iniciar una nueva operación de actualización de instancia	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SuspendProcesses	Concede permiso para suspender los procesos de Auto Scaling especificados, o todos los procesos, para el grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	Concede permiso para terminar la instancia especificada y, de forma opcional, ajusta el tamaño del grupo deseado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateAutoScalingGroup	Concede permiso para actualizar la configuración del grupo de Auto Scaling especificado.	Escritura	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:MaxSize	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				autoscaling:MinSize autoscaling:VPCZoneIdentifiers	

Tipos de recursos definidos por Amazon EC2 Auto Scaling

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
autoScalingGroup	`arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}`	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}
launchConfiguration	`arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${Id}:launchConfigurationName/${LaunchConfigurationName}`	

Claves de condición de Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
autoscaling:CapacityReservationIds	Filtra el acceso en función de la reserva de capacidad IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	Filtra el acceso en función del ARN de un grupo de recursos de reserva de capacidad	ArrayOfString
autoscaling:ImageId	Filtra el acceso en función del ID de AMI de la configuración de lanzamiento	Cadena
autoscaling:InstanceType	Filtra el acceso en función del tipo de instancia de la configuración de lanzamiento	Cadena
autoscaling:InstanceTypes	Filtra el acceso en función de los tipos de instancias presentes como anulaciones de una plantilla de lanzamiento de una política de instancias mixtas. Se utiliza para determinar qué tipos de instancias se pueden definir de manera explícita en la política	Cadena
autoscaling:LaunchConfigurationName	Filtra el acceso según el nombre de una configuración de lanzamiento.	Cadena

Claves de condición	Descripción	Tipo
autoscaling:LaunchTemplateVersionSpecified	Filtra el acceso en función de si los usuarios pueden especificar cualquier versión de una plantilla de lanzamiento o solo la versión más reciente o predeterminada.	Bool
autoscaling:LoadBalancerNames	Filtra el acceso según el nombre del equilibrador de carga.	ArrayOfString
autoscaling:MaxSize	Filtra el acceso en función del tamaño máximo de escalado de la solicitud	Numérico
autoscaling:MetadataHttpEndpoint	Filtra el acceso en función de si el punto de enlace de HTTP está o no habilitado para el servicio de metadatos de instancia.	Cadena
autoscaling:MetadataHttpPutResponseHopLimit	Filtra el acceso según la cantidad permitida de saltos al llamar al servicio de metadatos de instancia.	Numérico
autoscaling:MetadataHttpTokens	Filtra el acceso en función de si se requieren tokens al llamar al servicio de metadatos de instancia (opcional u obligatorio).	Cadena
autoscaling:MinSize	Filtra el acceso en función del tamaño mínimo de escalado de la solicitud	Numérico
autoscaling:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
autoscaling:SpotPrice	Filtra el acceso en función del precio de las instancias de spot de la configuración de lanzamiento	Numérico

Claves de condición	Descripción	Tipo
autoscaling:TargetGroupARNs	Filtra el acceso según el ARN de un grupo de destino.	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	Filtra el acceso en función de los identificadores de los orígenes de tráfico	ArrayOfString
autoscaling:VPCZoneIdentifiers	Filtra el acceso según el identificador de una zona de VPC.	ArrayOfString
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon EC2 Image Builder

Amazon EC2 Image Builder (prefijo de servicio:`imagebuilder`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EC2 Image Builder
- Tipos de recursos definidos por Amazon EC2 Image Builder
- Claves de condición de Amazon EC2 Image Builder

Acciones definidas por Amazon EC2 Image Builder

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelImageCreation	Concede permiso para cancelar la creación de una imagen	Escritura	image*		
CancelLifecycleExecution	Concede permiso para cancelar la ejecución de un ciclo de vida	Escritura	lifecycleExecution*		
CreateComponent	Concede el permiso para crear un nuevo componente	Write	component*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateContainerRecipe	Concede permiso para crear una nueva receta de contenedor	Write	containerRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ecr:DescribeImages ecr:DescribeRepositories iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ssm:GetParameter
CreateDistributionConfiguration	Concede permiso para crear una nueva configuración de distribución	Write	distributionConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource ssm:GetParameter

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateImage	Concede permiso para crear una nueva imagen	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					imagebuilder:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateImagePipeline	Concede permiso para crear una canalización de imagen	Write	imagePipeline*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					imagebuilder:TagResource
CreateImageRecipe	Concede permiso para crear una nueva receta de imagen	Write	imageRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInfrastructureConfiguration	Concede permiso para crear una nueva configuración de infraestructura	Escritura	infrastructureConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:TagResource sns:Publish

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLifecyclePolicy	Concede permiso para crear una nueva política de ciclo de vida	Escritura	lifecyclePolicy*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	iam:PassRole imagebuilder:TagResource
CreateWorkflow	Concede permiso para crear un nuevo flujo de trabajo	Escritura	workflow*	aws:RequestTag/${TagKey} aws:TagKeys	imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteComponent	Concede el permiso para eliminar un componente.	Write	component*		
DeleteContainerRecipe	Concede permiso para eliminar una receta de contenedor	Write	containerRecipe*		
DeleteDistributionConfiguration	Concede permiso para eliminar la configuración de distribución	Write	distributionConfiguration*		
DeleteImage	Concede permiso para eliminar una imagen	Write	image*		
DeleteImagePipeline	Concede permiso para eliminar una canalización de imagen	Write	imagePipeline*		
DeleteImageRecipe	Concede permiso para eliminar una receta de imagen	Write	imageRecipe*		
DeleteInfrastructureConfiguration	Concede permiso para eliminar una configuración de infraestructura	Escritura	infrastructureConfiguration*		
DeleteLifecyclePolicy	Concede permiso para eliminar una política de ciclo de vida	Escritura	lifecyclePolicy*		
DeleteWorkflow	Concede permiso para eliminar un flujo de trabajo	Escritura	workflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetComponent	Concede permiso para ver detalles de un componente	Read	component*		kms:Decrypt
GetComponentPolicy	Concede permiso para ver la política de recursos asociada a un componente	Read	component*		
GetContainerRecipe	Concede permiso para ver detalles de una canalización de contenedor	Read	containerRecipe*		
GetContainerRecipePolicy	Concede permiso para ver la política de recursos asociada a una receta de contenedor	Read	containerRecipe*		
GetDistributionConfiguration	Concede permiso para ver detalles de una configuración de distribución	Read	distributionConfiguration*		
GetImage	Concede permiso para ver detalles de una imagen	Read	image*	aws:ResourceTag/${TagKey}	
GetImagePipeline	Concede permiso para ver detalles de una canalización de imagen	Read	imagePipeline*		
GetImagePolicy	Concede permiso para ver la política de recursos asociada a una imagen	Read	image*		
GetImageRecipe	Concede permiso para ver detalles de la receta de una imagen	Read	imageRecipe*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetImageRecipePolicy	Concede permiso para ver la política de recursos asociada a la receta de una imagen	Read	imageRecipe*		
GetInfrastructureConfiguration	Concede permiso para ver detalles de una configuración de infraestructura	Lectura	infrastructureConfiguration*		
GetLifecycleExecution	Concede permisos para ver los detalles de la ejecución de un ciclo de vida	Lectura	lifecycleExecution*		
GetLifecyclePolicy	Concede permiso para ver detalles sobre una política de ciclo de vida	Lectura	lifecyclePolicy*		
GetMarketplaceResource	Otorga permiso para recuperar el recurso proporcionado por Marketplace	Lectura	component*		
GetWorkflow	Concede permiso para ver los detalles de un flujo de trabajo	Lectura	workflow*		kms:Decrypt
GetWorkflowExecution	Concede permisos para ver los detalles de la ejecución de un flujo de trabajo	Lectura	workflowExecution*		
GetWorkflowStepExecution	Concede permisos para ver los detalles de la ejecución de un paso del flujo de trabajo	Lectura	workflowStepExecution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportComponent	Concede permiso para importar un nuevo componente	Escritura	component *	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportDiskImage	Otorga permiso para importar una imagen de disco	Escritura	imageVersion*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportVmImage	Concede permiso para importar una imagen	Escritura	imageVersion*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole
ListComponentBuildVersions	Concede permiso para enumerar las versiones de compilación de componentes en su cuenta	List	componentVersion*		
ListComponents	Concede permiso para enumerar las versiones de componente que pertenecen a o que se comparten con su cuenta	List			
ListContainerRecipes	Concede permiso para enumerar las recetas de contenedor que pertenecen a su cuenta o que se comparten con ella	List			
ListDistributionConfigurations	Concede permiso para enumerar las configuraciones de distribución de su cuenta	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListImageBuildVersions	Concede permiso para enumerar las versiones de compilación de imágenes en su cuenta	Enumeración	imageVersion*		
ListImagePackages	Concede permiso para devolver una lista de paquetes instalados en la imagen especificada	Enumeración	image*	aws:ResourceTag/${TagKey}	
ListImagePipelineImages	Concede permiso para devolver una lista de imágenes creadas por la canalización especificada	Enumeración	imagePipeline*		
ListImagePipelines	Concede permiso para enumerar las canalizaciones de imagen de su cuenta	List			
ListImageRecipes	Concede permiso para enumerar las recetas de imágenes que pertenecen a o que se comparten con la cuenta	Enumeración			
ListImageScanFindingAggregations	Concede permiso para enumerar las agregaciones en los resultados del escaneo de imagen de su cuenta	Enumeración	image imagePipeline		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListImageScanFindings	Concede permiso para enumerar los resultados del escaneo de imagen de las imágenes de su cuenta	Enumeración	image		inspector2:ListFindings
			imagePipeline		
ListImages	Concede permiso para enumerar las versiones de imágenes que pertenecen a o que se comparten con la cuenta	List			
ListInfrastructureConfigurations	Concede permiso para enumerar las configuraciones de infraestructura de la cuenta	Enumeración			
ListLifecycleExecutionResources	Concede permiso para enumerar los recursos para la ejecución de un ciclo de vida especificado	Enumeración	lifecycleExecution*		
ListLifecycleExecutions	Concede permiso para enumerar las ejecuciones de ciclos de vida para un recurso especificado	Enumeración	image		
			lifecyclePolicy		
ListLifecyclePolicies	Concede permiso para enumerar las políticas del ciclo de vida de su cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas para un recurso de Image Builder	Lectura	component	aws:ResourceTag/${TagKey}	
			containerRecipe	aws:ResourceTag/${TagKey}	
			distributionConfiguration	aws:ResourceTag/${TagKey}	
			image	aws:ResourceTag/${TagKey}	
			imagePipeline	aws:ResourceTag/${TagKey}	
			imageRecipe	aws:ResourceTag/${TagKey}	
			infrastructureConfiguration	aws:ResourceTag/${TagKey}	
			lifecyclePolicy	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workflow	aws:ResourceTag/${TagKey}	
ListWaitingWorkflowSteps	Concede permiso para enumerar los pasos del flujo de trabajo en espera para la cuenta de llamada	Enumeración			
ListWorkflowBuildVersions	Concede permiso para enumerar las versiones de compilación del flujo de trabajo en tu cuenta	Enumeración	workflowVersion*		
ListWorkflowExecutions	Concede permiso para enumerar las ejecuciones de flujo de trabajo para la imagen especificada	Enumeración	image*		
ListWorkflowStepExecutions	Concede permiso para enumerar las ejecuciones del paso del flujo de trabajo para el flujo de trabajo especificado	Enumeración	workflowExecution*		
ListWorkflows	Concede permiso para enumerar las versiones del flujo de trabajo que pertenecen a o que se comparten con la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutComponentPolicy	Concede permiso para establecer la política de recursos asociada a un componente	Permissions management	component*		
PutContainerRecipePolicy	Concede permiso para establecer la política de recursos asociada a una receta de contenedor	Permissions management	containerRecipe*		
PutImagePolicy	Concede permiso para establecer la política de recursos asociada a una imagen	Permissions management	image*		
PutImageRecipePolicy	Concede permiso para establecer la política de recursos asociada a una receta de imagen	Administración de permisos	imageRecipe*		
SendWorkflowStepAction	Concede permiso para enviar una acción a un paso del flujo de trabajo	Escritura	image* workflowStepExecution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImagePipelineExecution	Concede permiso para crear una nueva imagen a partir de una canalización	Escritura	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
StartResourceStateUpdate	Concede permiso para iniciar una actualización del estado para el recurso especificado	Escritura	image*		
TagResource	Concede permiso para etiquetar un recurso de Image Builder	Etiquetado	component	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			containerRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			distributionConfiguration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			image	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			imagePipeline	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			imageRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			infrastructureConfiguration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			lifecyclePolicy	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workflow	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para desetiquetar un recurso de Image Builder	Etiquetado	component	aws:ResourceTag/${TagKey} aws:TagKeys	
			containerRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	
			distributionConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			image	aws:ResourceTag/${TagKey} aws:TagKeys	
			imagePipeline	aws:ResourceTag/${TagKey} aws:TagKeys	
			imageRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	
			infrastructureConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			lifecyclePolicy	aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workflow	aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDistributionConfiguration	Concede permiso para actualizar una configuración de distribución existente	Write	distributionConfiguration*		ssm:GetParameter

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateImagePipeline	Concede permiso para actualizar una canalización de imágenes existente	Write	imagePipeline*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateInfrastructureConfiguration	Concede permiso para actualizar una configuración de infraestructura existente	Escritura	infrastructureConfiguration*	aws:ResourceTag/${TagKey} imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:PassRole sns:Publish
UpdateLifecyclePolicy	Concede permisos para actualizar una política de ciclo de vida existente	Escritura	lifecyclePolicy*	imagebuilder:LifecyclePolicyResourceType	iam:PassRole

Tipos de recursos definidos por Amazon EC2 Image Builder

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
component	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}`	aws:ResourceTag/${TagKey}
componentVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}`	aws:ResourceTag/${TagKey}
distributionConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}`	aws:ResourceTag/${TagKey}
imageVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}`	aws:ResourceTag/${TagKey}
imageRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
containerRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}	aws:ResourceTag/${TagKey}
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
workflowExecution	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}`	
workflowStepExecution	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}`	

Claves de condición de Amazon EC2 Image Builder

Amazon EC2 Image Builder define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
imagebuilder:Creat	Filtra el acceso en función de los pares clave-valor de etiqueta adjuntados al recurso creado por Image Builder	Cadena

Claves de condición	Descripción	Tipo
edResourceTag/<key>		
imagebuilder:CreatedResourceTagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	Filtra el acceso según el requisito de token HTTP de los metadatos de la EC2 instancia especificado en la solicitud	Cadena
imagebuilder:LifecyclePolicyResourceType	Filtra el acceso por el tipo de recurso de la política de ciclo de vida especificado en la solicitud	Cadena
imagebuilder:StatusTopicArn	Filtra el acceso por el ARN de tema SNS en la solicitud en la que se publicarán las notificaciones de estado del terminal	ARN

Acciones, recursos y claves de condición de Amazon EC2 Instance Connect

Amazon EC2 Instance Connect (prefijo de servicio:`ec2-instance-connect`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EC2 Instance Connect
- Tipos de recursos definidos por Amazon EC2 Instance Connect
- Claves de condición de Amazon EC2 Instance Connect

Acciones definidas por Amazon EC2 Instance Connect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
OpenTunnel	Otorga permiso para establecer una conexión SSH a una EC2 EC2 instancia mediante Instance Connect Endpoint	Escritura	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ec2-instance-connect:privateIpAddress ec2-instance-connect:MaxTunnelDuration	
SendSSHPublicKey	Otorga permiso para enviar una clave pública de SSH a la EC2 instancia especificada para usarla en el SSH estándar	Escritura	instance*		
				ec2:osuser	
SendSerialConsoleSSHPublicKey	Otorga permiso para enviar una clave pública de SSH a la EC2 instancia especificada para utilizarla en el SSH de la consola en serie	Escritura	instance*		

Tipos de recursos definidos por Amazon EC2 Instance Connect

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}
instance-connect-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Claves de condición de Amazon EC2 Instance Connect

Amazon EC2 Instance Connect define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
ec2-instance-connect:maxTunnelDuration	Filtra el acceso según la duración máxima de la sesión asociada a la instancia	Numérico

Claves de condición	Descripción	Tipo
ec2-instance-connect:privateIpAddress	Filtra el acceso por la dirección IP privada asociada a la instancia	IPAddress
ec2-instance-connect:remotePort	Filtra el acceso por el número de puerto asociado a el recurso	Numérico
ec2:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
ec2:osuser	Filtra el acceso especificando el nombre de usuario predeterminado para la AMI utilizada para lanzar la instancia.	Cadena

Acciones, recursos y claves de condición para Amazon EKS Auth

Amazon EKS Auth (prefijo de servicio: `eks-auth`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EKS Auth
- Tipos de recursos definidos por Amazon EKS Auth
- Claves de condición para Amazon EKS Auth

Acciones definidas por Amazon EKS Auth

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssumeRoleForPodIdentity	Otorga permiso para intercambiar un token de cuenta de servicio de Kubernetes por credenciales temporales AWS	Lectura	cluster*		

Tipos de recursos definidos por Amazon EKS Auth

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon EKS Auth

Amazon EKS Auth define las siguientes claves de condición que se pueden usar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena

Acciones, recursos y claves de condición para AWS Elastic Beanstalk

AWS Elastic Beanstalk (`elasticbeanstalk`prefijo de servicio:) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Elastic Beanstalk
- Tipos de recursos definidos por AWS Elastic Beanstalk
- Claves de condición para AWS Elastic Beanstalk

Acciones definidas por AWS Elastic Beanstalk

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AbortEnvironmentUpdate	Otorga permiso para cancelar una actualización de configuración del entorno en curso o la implementación de una versión de la aplicación	Escritura	environment*	elasticbeanstalk:InApplication	
AddTags	Otorga permiso para agregar etiquetas a un recurso de Elastic Beanstalk y para actualizar valores de etiqueta	Etiquetado	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ApplyEnvironmentManagedAction	Otorga permiso para aplicar una acción administrada programada de forma inmediata	Escritura	environment*	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateEnvironmentOperationsRole	Otorga permiso para asociar un rol de operaciones a un entorno	Escritura	environment*		
CheckDNSAvailability	Otorga permiso para verificar la disponibilidad de CNAME	Lectura			
ComposeEnvironments	Otorga permiso para crear o actualizar un grupo de entornos, cada uno de ellos ejecutando un componente distinto de una sola aplicación	Escritura	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	Otorga permiso para crear una aplicación nueva	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationVersion	Otorga permiso para crear una versión de la aplicación para una aplicación	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	Otorga permiso para crear una plantilla de configuración	Escritura	configurationtemplate*	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Otorga permiso para lanzar un entorno para una aplicación	Escritura	environment*	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	Otorga permiso para crear una nueva versión de una plataforma personalizada	Escritura	platform*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	Otorga permiso para crear la ubicación de almacenamiento de Amazon S3 para la cuenta	Escritura			
DeleteApplication	Otorga permiso para eliminar una aplicación junto con todas las versiones y configuraciones asociadas	Escritura	application*		
DeleteApplicationVersion	Otorga permiso para eliminar una versión de la aplicación de una aplicación	Escritura	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	Otorga permiso para eliminar una plantilla de configuración	Escritura	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	Otorga permiso para eliminar la configuración provisional asociada al entorno en ejecución	Escritura	environment*	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePlatformVersion	Otorga permiso para eliminar una versión de una plataforma personalizada	Escritura	platform*		
DescribeAccountAttributes	Otorga permiso para recuperar una lista de atributos de la cuenta, lo que incluye cuotas de recursos	Lectura			
DescribeApplicationVersions	Otorga permiso para recuperar una lista de versiones de aplicaciones almacenadas en un depósito de almacenamiento de AWS Elastic Beanstalk	Enumeración	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	Otorga permiso para recuperar las descripciones de las aplicaciones existentes	Enumeración	application		
DescribeConfigurationOptions	Otorga permiso para recuperar las descripciones de las opciones de configuración del entorno	Lectura	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
			solutionstack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConfigurationSettings	Otorga permiso para recuperar una descripción de la configuración de un conjunto de configuración	Lectura	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	Otorga permiso para recuperar información sobre el estado general de un entorno	Lectura	environment		
DescribeEnvironmentManagedActionHistory	Otorga permiso para recuperar una lista de acciones administradas completadas y con error de un entorno	Lectura	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	Otorga permiso para recuperar una lista de acciones administradas en curso e inminentes de un entorno	Lectura	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentResources	Otorga permiso para recuperar una lista de AWS recursos para un entorno	Lectura	environment	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEnvironments	Otorga permiso para recuperar las descripciones de los entornos existentes	Enumeración	environment	elasticbeanstalk:InApplication	
DescribeEvents	Otorga permiso para recuperar una lista de descripciones de eventos que se corresponden con un conjunto de criterios	Lectura	application		
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	Otorga permiso para recuperar información más detallada sobre el estado de las instancias del entorno	Lectura	environment		
DescribePlatformVersion	Concede permiso para recuperar una descripción de una versión de la plataforma administrada	Lectura	platform		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateEnvironmentOperationsRole	Otorga permiso para desasociar un rol de operaciones de un entorno	Escritura	environment*		
ListAvailableSolutionStacks	Otorga permiso para recuperar una lista de los nombres de pila de soluciones disponibles	Enumeración	solutionstack		
ListPlatformBranches	Otorga permiso para recuperar una lista de las ramas de la plataforma disponibles	Enumeración			
ListPlatformVersions	Otorga permiso para recuperar una lista de las plataformas disponibles	Enumeración	platform		
ListTagsForResource	Otorga permiso para recuperar una lista de etiquetas de un recurso de Elastic Beanstalk	Lectura	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutInstanceStatistics	Otorga permiso para enviar estadísticas de instancia para mejorar el estado	Escritura	application*		
			environment*		
RebuildEnvironment	Otorga permiso para eliminar y volver a crear todos los AWS recursos de un entorno y para forzar un reinicio	Escritura	environment*	elasticbeanstalk:InApplication	
RemoveTags	Otorga permiso para eliminar etiquetas de un recurso de Elastic Beanstalk	Etiquetado	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:TagKeys	
RequestEnvironmentInfo	Otorga permiso para iniciar una solicitud para compilar información del entorno implementado	Lectura	environment*	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestartAppServer	Otorga permiso para solicitar un entorno para reiniciar el servidor contenedor de aplicaciones que se ejecuta en cada EC2 instancia de Amazon	Escritura	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	Otorga permiso para recuperar la información compilada de una RequestEnvironmentInfo solicitud	Lectura	environment*	elasticbeanstalk:InApplication	
SwapEnvironmentCNAMEs	Otorga permiso para intercambiar dos entornos CNAMEs	Escritura	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	Otorga permiso para terminar un entorno	Escritura	environment*	elasticbeanstalk:InApplication	
UpdateApplication	Otorga permiso para actualizar una aplicación con propiedades especificadas	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApplicationResourceLifecycle	Otorga permiso para actualizar la política de ciclo de vida de la versión de la aplicación asociada con la aplicación	Escritura	application*		
UpdateApplicationVersion	Otorga permiso para actualizar una versión de la aplicación con propiedades especificadas	Escritura	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	Otorga permiso para actualizar una plantilla de configuración con los valores de las opciones de configuración o propiedades que se especifican	Escritura	configurationtemplate*	elasticbeanstalk:InApplication	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEnvironment	Otorga permiso para actualizar un entorno.	Escritura	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTagsForResource	No concede permiso para actualizar etiquetas. Para conceder permiso para añadir etiquetas a un recurso de Elastic Beanstalk, eliminar etiquetas y actualizar sus valores, especifique elasticbeanstalk: y elasticbeanstalk: AddTags RemoveTags	Etiquetado	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	Otorga permiso para verificar la validez de un conjunto de opciones de configuración para una plantilla de configuración o un entorno	Lectura	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Tipos de recursos definidos por AWS Elastic Beanstalk

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
applicationversion	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:applicationversion/${ApplicationName}/${VersionLabel}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
configurationtemplate	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:configurationtemplate/${ApplicationName}/${TemplateName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
environment	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:environment/${ApplicationName}/${EnvironmentName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
solutionstack	`arn:${Partition}:elasticbeanstalk:${Region}::solutionstack/${SolutionStackName}`	

Tipos de recurso	ARN	Claves de condición
platform	`arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}`	

Claves de condición para AWS Elastic Beanstalk

AWS Elastic Beanstalk define las siguientes claves de condición que se pueden utilizar `Condition` en el elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString
elasticbeanstalk:FromApplication	Filtra el acceso por una aplicación como una dependencia o una restricción en un parámetro de entrada	ARN
elasticbeanstalk:FromApplicationVersion	Filtra el acceso por una versión de la aplicación como una dependencia o una restricción en un parámetro de entrada	ARN

Claves de condición	Descripción	Tipo
elasticbeanstalk:FromConfigurationTemplate	Filtra el acceso por una plantilla de configuración como una dependencia o una restricción en un parámetro de entrada	ARN
elasticbeanstalk:FromEnvironment	Filtra el acceso por un entorno como una dependencia o una restricción en un parámetro de entrada	ARN
elasticbeanstalk:FromPlatform	Filtra el acceso por una plataforma como una dependencia o una restricción en un parámetro de entrada	ARN
elasticbeanstalk:FromSolutionStack	Filtra el acceso por una pila de soluciones como una dependencia o una restricción en un parámetro de entrada	ARN
elasticbeanstalk:InApplication	Filtra el acceso por la aplicación que contiene el recurso en el que opera la acción	ARN

Acciones, recursos y claves de condición para Amazon Elastic Block Store

Amazon Elastic Block Store (prefijo de servicio: `ebs`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic Block Store
- Tipos de recursos definidos por Amazon Elastic Block Store
- Claves de condición para Amazon Elastic Block Store

Acciones definidas por Amazon Elastic Block Store

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CompleteSnapshot	Otorga permiso para sellar y completar la instantánea después de que se hayan escrito todos los bloques de datos requeridos en ella	Escritura	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Otorga permiso para devolver los datos de un bloque en una instantánea de Amazon Elastic Block Store (EBS).	Lectura	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	Otorga permiso para enumerar los bloques que son diferentes entre dos instantáneas de Amazon Elastic Block Store (EBS) del mismo linaje volume/snapshot	Lectura	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	Otorga permiso para enumerar los bloques en	Lectura	snapshot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	una instantánea de Amazon Elastic Block Store (EBS)			aws:ResourceTag/${TagKey}	
PutSnapshotBlock	Otorga permiso para escribir un bloque de datos en una instantánea creada por la operación StartSnapshot	Escritura	snapshot*		
				aws:ResourceTag/${TagKey}	
StartSnapshot	Otorga permiso para crear una nueva instantánea de EBS	Escritura	snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Tipos de recursos definidos por Amazon Elastic Block Store

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Claves de condición para Amazon Elastic Block Store

Amazon Elastic Block Store define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
ebs:Description	Filtra el acceso según la descripción de la instantánea que se está creando	Cadena
ebs:ParentSnapshot	Filtra el acceso según el ID de la instantánea principal	Cadena
ebs:VolumeSize	Filtra el acceso según el tamaño del volumen para la instantánea que se está creando, en GiB	Numérico

Acciones, recursos y claves de condición para Amazon Elastic Container Registry

Amazon Elastic Container Registry (prefijo de servicio: `ecr`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic Container Registry
- Tipos de recursos definidos por Amazon Elastic Container Registry
- Claves de condición para Amazon Elastic Container Registry

Acciones definidas por Amazon Elastic Container Registry

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchCheckLayerAvailability	Concede permiso para comprobar la disponibilidad de varias capas de imagen en un registro y repositorio especificados	Read	repository*		
BatchDeleteImage	Concede permiso para eliminar una lista de imágenes especificadas dentro de un repositorio especificado	Write	repository*		
BatchGetImage	Concede permiso para obtener información detallada de imágenes especificadas dentro de un repositorio especificado	Lectura	repository*		
BatchGetRepositoryScanningConfiguration	Concede permiso para recuperar la configuración de escaneo de repositorios para una lista de repositorios.	Lectura	repository*		
BatchImportUpstrea	Concede permiso para recuperar la imagen del registro ascendente e	Escritura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
mImage [solo permiso]	importarla a su registro privado				
CompleteLayerUpload	Concede permiso para informar a Amazon ECR de que la carga de capa de imagen para un registro especificado, nombre de repositorio e ID de carga se ha completado.	Escritura	repository*		
CreatePullThroughCacheRule	Concede permiso para crear una nueva regla de caché de extracción.	Escritura			iam:CreateServiceLinkedRole
CreateRepository	Concede permiso para crear un repositorio de imágenes	Escritura	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRepositoryCreationTemplate	Concede permiso para crear la plantilla de creación de repositorio	Escritura			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
DeleteLifecyclePolicy	Concede permiso para eliminar la política de ciclo de vida especificada	Escritura	repository*		
DeletePullThroughCacheRule	Concede permiso para eliminar la regla de caché de extracción.	Escritura			
DeleteRegistryPolicy	Concede permiso para eliminar la política del registro	Administración de permisos			
DeleteRepository	Concede permiso para eliminar un repositorio de imágenes existente	Escritura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRepositoryCreationTemplate	Concede permiso para eliminar la plantilla de creación de repositorio	Escritura			
DeleteRepositoryPolicy	Concede permiso para eliminar la política de repositorio de un repositorio especificado	Administración de permisos	repository*		
DescribeImageReplicationStatus	Concede permiso para recuperar el estado de replicación de una imagen en un registro, incluido el motivo del error si la replicación falla	Lectura	repository*		
DescribeImageScanFindings	Concede permiso para describir los resultados del escaneo de imagen de la imagen especificada	Read	repository*		
DescribeImages	Concede permiso para obtener los metadatos de las imágenes de un repositorio, entre los que se incluyen tamaño de imagen, etiquetas de imagen y fecha de creación.	Enumeración	repository*		
DescribePullThroughCacheRules	Concede permiso para describir las reglas de caché de extracción.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRegistry	Concede permiso para describir la configuración del registro	Read			
DescribeRepositories	Concede permiso para describir repositorios de imágenes en un registro	Lectura	repository*		
DescribeRepositoryCreationTemplates	Concede permiso para describir la plantilla de creación de repositorio	Lectura			
GetAccountSetting	Concede permiso para obtener la configuración de la cuenta	Lectura		ecr:AccountSetting	
GetAuthorizationToken	Concede permiso para recuperar un token válido para un registro especificado durante 12 horas	Read			
GetDownloadUrlForLayer	Concede permiso para recuperar la URL de descarga correspondiente a una capa de imagen	Lectura	repository*		
GetImageCopyStatus [solo permiso]	Otorga permiso para recuperar el estado de una copia de imagen	Lectura	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLifecyclePolicy	Concede permiso para recuperar la política de ciclo de vida especificada	Read	repository*		
GetLifecyclePolicyPreview	Concede permiso para recuperar los resultados de la solicitud de vista previa de la política de ciclo de vida especificada	Read	repository*		
GetRegistryPolicy	Concede permiso para recuperar la política del registro	Lectura			
GetRegistryScanningConfiguration	Concede permiso para recuperar la configuración de análisis del registro.	Lectura			
GetRepositoryPolicy	Concede permiso para recuperar la política de repositorio para un repositorio especificado	Read	repository*		
InitiateLayerUpload	Concede permiso para notificar a Amazon ECR que tiene la intención de cargar una capa de imagen	Escritura	repository*		
ListImages	Otorga permiso para enumerar todas las imágenes IDs de un repositorio determinado	Enumeración	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para publicar las etiquetas de un recurso de Amazon ECR	Lectura	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAccountSetting	Concede permiso para actualizar la configuración de la cuenta	Escritura		ecr:AccountSetting	
PutImage	Concede permiso para crear o actualizar el manifiesto de imagen asociado a una imagen	Write	repository*		
PutImageScanningConfiguration	Concede permiso para actualizar la configuración de escaneo de imágenes para un repositorio	Write	repository*		
PutImageTagMutability	Concede permiso para actualizar la configuración de mutabilidad de etiquetas de imagen para un repositorio	Write	repository*		
PutLifecyclePolicy	Concede permiso para crear o actualizar una política de ciclo de vida	Write	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutRegistryPolicy	Concede permiso para actualizar la política del registro	Administración de permisos			
PutRegistryScanningConfiguration	Concede permiso para actualizar la configuración de análisis del registro.	Escritura			
PutReplicationConfiguration	Concede permiso para actualizar la configuración de replicación del registro	Escritura			iam:CreateServiceLinkedRole
ReplicateImage [solo permiso]	Concede permiso para replicar imágenes en el registro de destino	Write	repository*		
SetRepositoryPolicy	Concede permiso para aplicar una política de repositorio en un repositorio especificado para controlar los permisos de acceso	Permissions management	repository*		
StartImageScan	Concede permiso para iniciar un análisis de imagen	Write	repository*		
StartLifecyclePolicyPreview	Concede permiso para iniciar una vista previa de la política de ciclo de vida especificada	Write	repository*		
TagResource	Concede permiso para etiquetar un recurso de Amazon ECR	Etiquetado	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para desetiquetar un recurso de Amazon ECR	Etiquetado	repository*		
				aws:TagKeys	
UpdatePullThroughCacheRule	Concede permiso para actualizar la regla de caché de extracción	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRepositoryCreationTemplate	Concede permiso para actualizar la plantilla de creación de repositorios	Escritura			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
UploadLayerPart	Concede permiso para cargar una parte de capa de imagen a Amazon ECR	Escritura	repository*		
ValidatePullThroughCacheRule	Concede permiso para validar la regla de caché de extracción	Lectura			

Tipos de recursos definidos por Amazon Elastic Container Registry

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
repository	`arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Claves de condición para Amazon Elastic Container Registry

Amazon Elastic Container Registry define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
ecr:AccountSetting	Filtra el acceso por el nombre de configuración de la cuenta ECR	Cadena

Claves de condición	Descripción	Tipo
ecr:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena

Acciones, recursos y claves de condición de Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public (prefijo de servicio: `ecr-public`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic Container Registry Public
- Tipos de recursos definidos por Amazon Elastic Container Registry Public
- Claves de condición para Amazon Elastic Container Registry Public

Acciones definidas por Amazon Elastic Container Registry Public

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchCheckLayerAvailability	Concede permiso para comprobar la disponibilidad de varias capas de imagen en un registro y repositorio especificados	Read	repository*		
BatchDeleteImage	Concede permiso para eliminar una lista de imágenes especificadas dentro de un repositorio especificado	Write	repository*		
CompleteLayerUpload	Concede permiso para informar a Amazon ECR de que la carga de capa de imagen para un registro especificado, nombre de repositorio e ID de carga se ha completado.	Write	repository*		
CreateRepository	Concede permiso para crear un repositorio de imágenes	Write	repository*		ecr-public:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRepository	Otorga permisos para eliminar un repositorio de imágenes existente	Write	repository*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRepositoryPolicy	Otorga permisos para eliminar la política de repositorio de un repositorio especificado	Write	repository*		
DescribeImageTags	Otorga permiso para describir todas las etiquetas de imágenes de un repositorio determinado	List	repository*		
DescribeImages	Otorga permisos para obtener los metadatos de las imágenes de un repositorio, entre los que se incluyen tamaño de imagen, etiquetas de imagen y fecha de creación.	Read	repository*		
DescribeRegistries	Otorga permiso para recuperar los datos de catálogo asociados a un registro	List	registry*		
DescribeRepositories	Otorga permisos para describir repositorios de imágenes en un registro	List	repository		
GetAuthorizationToken	Otorga permisos para recuperar un token válido para un registro especificado durante 12 horas	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRegistryCatalogData	Otorga permiso para recuperar los datos de catálogo asociados a un registro	Read	registry*		
GetRepositoryCatalogData	Otorga permiso para recuperar los datos de catálogo asociados a un repositorio	Read	repository*		
GetRepositoryPolicy	Concede permiso para recuperar la política de repositorio para un repositorio especificado	Read	repository*		
InitiateLayerUpload	Concede permiso para notificar a Amazon ECR que tiene la intención de cargar una capa de imagen	Write	repository*		
ListTagsForResource	Otorga permisos para publicar las etiquetas de un recurso de Amazon ECR	Read	repository*		
PutImage	Concede permiso para crear o actualizar el manifiesto de imagen asociado a una imagen	Write	repository*		
PutRegistryCatalogData	Otorga permiso para crear y actualizar los datos de catálogo asociados a un registro	Write	registry*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutRepositoryCatalogData	Otorga permiso para actualizar los datos de catálogo asociados a un repositorio	Write	repository*		
SetRepositoryPolicy	Concede permiso para aplicar una política de repositorio en un repositorio especificado para controlar los permisos de acceso	Permissions management	repository*		
TagResource	Otorga permisos para etiquetar un recurso de Amazon ECR	Etiquetado	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para desetiquetar un recurso de Amazon ECR	Etiquetado	repository*		
				aws:TagKeys	
UploadLayerPart	Otorga permiso para cargar una parte de la capa de imagen en Amazon ECR Public	Write	repository*		

Tipos de recursos definidos por Amazon Elastic Container Registry Public

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
repository	`arn:${Partition}:ecr-public::${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr-public:ResourceTag/${TagKey}
registry	`arn:${Partition}:ecr-public::${Account}:registry/${RegistryId}`	

Claves de condición para Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra solicitudes de creación en función del conjunto de valores permitido para cada una de las etiquetas.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado al recurso	Cadena
aws:TagKeys	Filtra las solicitudes de creación según la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
ecr-public:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado al recurso	Cadena

Claves de condición, recursos y acciones de Amazon Elastic Container Service

Amazon Elastic Container Service (prefijo de servicio: `ecs`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic Container Service
- Tipos de recursos definidos por Amazon Elastic Container Service
- Claves de condición de Amazon Elastic Container Service

Acciones definidas por Amazon Elastic Container Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCapacityProvider	Concede permiso para crear un nuevo proveedor de capacidad. Los proveedores de capacidad están asociados a un clúster de Amazon ECS y se utilizan en estrategias de proveedores de capacidad para facilitar el escalado automático de clústeres.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Concede permiso para crear un nuevo clúster de Amazon ECS.	Write	cluster*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:fargate-ephemeral-stora	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ge-kms-key	
CreateService	Concede permiso para ejecutar y mantener el número deseado de tareas a partir de una definición de tarea especificada mediante la creación de servicios.	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:task-definition ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace ecs:enable-vpc-lattice	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ecs:enable-ecs-managed-tags ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTaskSet	Concede permiso para crear un nuevo conjunto de tareas de Amazon ECS.	Write		aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:service ecs:task-definition	
DeleteAccountSetting	Concede permiso para modificar el formato ARN y de ID de recurso de un recurso para un usuario de IAM especificado, un rol de IAM o el usuario raíz de una cuenta. Puede especificar si el nuevo formato de ID y ARN del recurso está deshabilitado para los nuevos recursos que se crean.	Write		ecs:account-setting	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAttributes	Concede permiso para eliminar uno o varios atributos personalizados de un recurso de Amazon ECS.	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteCapacityProvider	Concede permiso para eliminar el proveedor de capacidad especificado.	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DeleteCluster	Concede permiso para eliminar el clúster especificado.	Write	cluster*	aws:ResourceTag/${TagKey}	
DeleteService	Concede permiso para eliminar un servicio especificado dentro de un clúster.	Escritura	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTaskDefinitions	Concede permiso para anular las definiciones de tarea especificada por familia y revisión	Escritura	task-definition*		
				aws:ResourceTag/${TagKey}	
DeleteTaskSet	Concede permiso para eliminar el conjunto de tareas especificado.	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DeregisterContainerInstance	Concede permiso para anular el registro de una instancia de contenedor de Amazon ECS desde el clúster especificado.	Write	cluster*	aws:ResourceTag/${TagKey}	
DeregisterTaskDefinition	Concede permiso para anular el registro de la definición de tarea especificada por familia y revisión.	Write			
DescribeCapacityProviders	Concede permiso para describir uno o varios proveedores de capacidad de Amazon ECS.	Read	capacity-provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DescribeClusters	Concede permiso para describir uno o varios de los clústeres.	Read	cluster*	aws:ResourceTag/${TagKey}	
DescribeContainerInstances	Concede permiso para describir instancias de contenedor de Amazon ECS.	Lectura	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeServiceDeployments	Otorga permiso para describir una o más de sus implementaciones de servicios	Lectura	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServiceRevisions	Otorga permiso para describir una o más de las revisiones del servicio	Lectura	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-revision*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServices	Concede permiso para describir los servicios especificados que se ejecutan en el clúster.	Read	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeTaskDefinition	Concede permiso para describir una definición de tarea. Puede especificar una familia y una revisión con el fin de buscar información sobre una definición de tarea específica o puede especificar simplemente la familia para encontrar la última revisión ACTIVE en esa familia.	Read			
DescribeTaskSets	Concede permiso para describir los conjuntos de tareas de Amazon ECS.	Read	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DescribeTasks	Concede permiso para describir una tarea o tareas especificadas.	Read	task*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ecs:cluster	
DiscoverPollEndpoint	Concede permiso para obtener un punto de enlace para que el agente de Amazon ECS sondee con el objetivo de buscar actualizaciones.	Write			
ExecuteCommand	Concede permiso para ejecutar un comando de forma remota en un contenedor de Amazon ECS.	Escritura	cluster* task*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:container-name ecs:task	
GetTaskProtection	Concede permiso para recuperar el estado de protección de las tareas en un servicio Amazon ECS	Lectura	task*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ecs:cluster	
ListAccountSettings	Concede permiso para enumerar la configuración de la cuenta de un recurso de Amazon ECS para una entidad principal especificada.	Read			
ListAttributes	Concede permiso para enumerar los atributos de los recursos de Amazon ECS dentro de un clúster y un tipo de destino especificados.	List	cluster*	aws:ResourceTag/${TagKey}	
ListClusters	Concede permiso para obtener una lista de clústeres existentes.	List			
ListContainerInstances	Concede permiso para obtener una lista de instancias de contenedor en un clúster especificado.	Enumeración	cluster*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServiceDeployments	Otorga permiso para obtener una lista de las implementaciones de servicios para un servicio específico	Enumeración	service*	aws:ResourceTag/${TagKey} ecs:cluster	
ListServices	Concede permiso para obtener una lista de servicios que se ejecutan en un clúster especificado.	Enumeración		ecs:cluster	
ListServicesByNamespace	Otorga permiso para obtener una lista de los servicios que se ejecutan en un espacio de nombres de Nube de AWS mapas específico	Enumeración		ecs:namespace	
ListTagsForResource	Concede permiso para obtener una lista de etiquetas del recurso especificado.	Read	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ListTaskDefinitionFamilies	Concede permiso para obtener una lista de familias de definición de tareas registradas en su cuenta (que pueden incluir familias de definición de tareas que ya no tienen definiciones de tareas ACTIVE)	List			
ListTaskDefinitions	Concede permiso para obtener una lista de definiciones de tareas registradas en su cuenta.	List			
ListTasks	Concede permiso para obtener una lista de tareas para un clúster especificado.	List	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Poll [solo permiso]	Concede permiso a un agente para conectarse con el servicio Amazon ECS con el fin de informar sobre el estado y obtener comandos.	Write	container-instance*		
				ecs:cluster	
PutAccountSetting	Concede permiso para modificar el formato ARN y de ID de recurso de un recurso para un usuario de IAM especificado, un rol de IAM o el usuario raíz de una cuenta. Puede especificar si el nuevo formato de ID y ARN del recurso está habilitado o para los nuevos recursos que se creen. La habilitación de esta configuración es necesaria para utilizar nuevas características de Amazon ECS, como el etiquetado de recursos.	Write		ecs:account-setting	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutAccountSettingDefault	Concede permiso para modificar el formato ARN e ID de recurso de un tipo de recurso a todos los usuarios de IAM de una cuenta para la que no se haya establecido ninguna configuración de cuenta individual. La habilitación de esta configuración es necesaria para utilizar nuevas características de Amazon ECS, como el etiquetado de recursos.	Write		ecs:account-setting	
PutAttributes	Concede permiso para crear o actualizar un atributo en un recurso de Amazon ECS.	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
PutClusterCapacityProviders	Concede permiso para modificar los proveedores de capacidad disponibles y la estrategia predeterminada de proveedor de capacidad para un clúster.	Escritura	cluster*	aws:ResourceTag/${TagKey}	
				ecs:capacity-provider	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterContainerInstance	Otorga permiso para registrar una EC2 instancia en el clúster especificado	Escritura	cluster*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterTaskDefinition	Concede permiso para registrar una nueva definición de tarea de la familia suministrada y containerDefinitions.	Write	task-definition*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys ecs:compute-compatibility ecs:privileged ecs:task-cpu ecs:task-memory	
RunTask	Concede permiso para iniciar una tarea mediante la colocación aleatoria y el programador predeterminado de Amazon ECS.	Write	task-definition*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartTask	Concede permiso para iniciar una nueva tarea a partir de la definición de tarea especificada en la instancia o instancias de contenedor especificadas.	Write	task-definition*		iam:PassRole
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:container-instances ecs:enable-ebs-volumes ecs:enable-execute-command	
StartTelemetrySession	Concede permiso para iniciar una sesión de telemetría.	Escritura	container-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ecs:cluster	
StopServiceDeployment	Otorga permiso para detener la implementación de un servicio en curso	Escritura	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
StopTask	Concede permiso para detener una tarea en ejecución.	Write	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
SubmitAttachmentStateChanges	Concede permiso para enviar una confirmación de que los archivos adjuntos cambiaron de estado.	Write	cluster*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SubmitContainerStateChange	Concede permiso para enviar una confirmación de que un contenedor cambió estados.	Write	cluster*	aws:ResourceTag/${TagKey}	
SubmitTaskStateChange	Concede permiso para enviar una confirmación de que una tarea cambió estados.	Write	cluster*	aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para etiquetar el recurso especificado	Etiquetado	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} ecs:CreateAction	
UntagResource	Concede permiso para quitar las etiquetas del recurso especificado	Etiquetado	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCapacityProvider	Concede permiso para actualizar el proveedor de capacidad especificado.	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	Concede permiso para modificar la configuración o ajustes que se van a utilizar para un clúster.	Write	cluster*	aws:ResourceTag/${TagKey}	
				ecs:fargate-ephemeral-storage-kms-key	
UpdateClusterSettings	Concede permiso con el fin de modificar la configuración que se va a utilizar para un clúster.	Write	cluster*	aws:ResourceTag/${TagKey}	
UpdateContainerAgent	Concede permiso para actualizar el agente de contenedor de Amazon ECS en una instancia de contenedor especificada.	Write	container-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateContainerInstancesState	Concede permiso al usuario para modificar el estado de una instancia de contenedor de Amazon ECS.	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateService	Concede permiso para modificar los parámetros de un servicio.	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace ecs:task-definition ecs:enable-vpc-lattice ecs:enable-ecs-managed-tags	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	
UpdateServicePrimaryTaskSet	Concede permiso para modificar el conjunto de tareas principal utilizado en un servicio.	Escritura	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskProtection	Concede permiso para modificar el estado de protección de una tarea	Escritura	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTaskSet	Concede permiso para actualizar el conjunto de tareas especificado.	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	

Tipos de recursos definidos por Amazon Elastic Container Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:ecs:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
container-instance	`arn:${Partition}:ecs:${Region}:${Account}:container-instance/${ClusterName}/${ContainerInstanceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
		ecs:ResourceTag/${TagKey}
service	arn:${Partition}:ecs:${Region}:${Account}:service/${ClusterName}/${ServiceName}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
service-deployment	arn:${Partition}:ecs:${Region}:${Account}:service-deployment/${ClusterName}/${ServiceName}/${ServiceDeploymentId}	aws:ResourceTag/${TagKey} ecs:cluster ecs:service
service-revision	arn:${Partition}:ecs:${Region}:${Account}:service-revision/${ClusterName}/${ServiceName}/${ServiceRevisionId}	aws:ResourceTag/${TagKey} ecs:cluster ecs:service
task	arn:${Partition}:ecs:${Region}:${Account}:task/${ClusterName}/${TaskId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task-definition	arn:${Partition}:ecs:${Region}:${Account}:task-definition/${TaskDefinitionFamilyName}:${TaskDefinitionRevisionNumber}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
capacity-provider	arn:${Partition}:ecs:${Region}:${Account}:capacity-provider/${CapacityProviderName}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task-set	arn:${Partition}:ecs:${Region}:${Account}:task-set/${ClusterName}/${ServiceName}/${TaskSetId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

Claves de condición de Amazon Elastic Container Service

Amazon Elastic Container Service define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
ecs:CreateAction	Filtra el acceso mediante el nombre de una acción de API que crea recursos	Cadena
ecs:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
ecs:account-setting	Filtra el acceso mediante el nombre de la configuración de la cuenta de Amazon ECS.	Cadena
ecs:auto-assign-public-ip	Filtra el acceso según la configuración de asignación de IP pública de su tarea de Amazon ECS o servicio de Amazon ECS que utiliza el modo de red awsvpc	Bool
ecs:capacity-provider	Filtra el acceso por el ARN de un proveedor de capacidad de Amazon ECS	ArrayOfARN
ecs:cluster	Filtra el acceso por el ARN de un clúster de Amazon ECS.	ARN
ecs:compute-compatibility	Filtra el acceso por el campo de compatibilidades obligatorio proporcionado en la solicitud	ArrayOfString
ecs:container-instances	Filtra el acceso por el ARN de una instancia de contenedor de Amazon ECS	ARN
ecs:container-name	Filtra el acceso por el nombre de un contenedor de Amazon ECS que se define en la definición de la tarea de ECS	Cadena
ecs:enable-ebs-volumes	Filtra el acceso por la capacidad de volumen de Amazon EBS administrado por Amazon ECS de la tarea o servicio de ECS	Cadena

Claves de condición	Descripción	Tipo
ecs:enable-ecs-managed-tags	Filtra el acceso mediante la configuración de habilitación de ECSManaged etiquetas de su tarea de Amazon ECS o servicio de Amazon ECS	Bool
ecs:enable-execute-command	Filtra el acceso por la capacidad de ejecución de comandos de su tarea de Amazon ECS o servicio de Amazon ECS	Cadena
ecs:enable-service-connect	Filtra el acceso por el valor del campo de habilitación en la configuración del servicio Connect	Cadena
ecs:enable-vpc-lattice	Filtra el acceso mediante la capacidad reticular de VPC de su servicio Amazon ECS	Cadena
ecs:fargate-ephemeral-storage-kms-key	Filtra el acceso por el identificador de clave de AWS KMS proporcionado en la solicitud	Cadena
ecs:namespace	Filtra el acceso por el ARN del espacio de nombres del Nube de AWS mapa, que se define en la configuración de Service Connect	ARN
ecs:privileged	Filtra el acceso por el campo privilegiado proporcionado en la solicitud	Cadena
ecs:propagate-tags	Filtra el acceso según la configuración de propagación de etiquetas de su tarea de Amazon ECS o servicio de Amazon ECS	Cadena
ecs:service	Filtra el acceso por el ARN de un servicio de Amazon ECS	ARN
ecs:subnet	Filtra el acceso según la configuración de subred de su tarea de Amazon ECS o servicio de Amazon ECS que utiliza el modo de red awsvpc	ArrayOfString

Claves de condición	Descripción	Tipo
ecs:task	Filtra el acceso por el ARN de una tarea de Amazon ECS	ARN
ecs:task-cpu	Filtra el acceso por la CPU de la tarea, como un entero con 1024 = 1 vCPU, proporcionado en la solicitud	Numérico
ecs:task-definition	Filtra el acceso por el ARN de una definición de tarea de Amazon ECS	ARN
ecs:task-memory	Filtra el acceso por la memoria de tareas, como un entero que representa MiB, proporcionado en la solicitud	Numérico

Acciones, recursos y claves de condición para AWS Elastic Disaster Recovery.

AWS Elastic Disaster Recovery (prefijo de servicio:`drs`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Recuperación de desastres
- Tipos de recurso definidos por AWS Elastic Disaster Recovery
- Claves de condición para AWS Elastic Disaster Recovery

Acciones definidas por AWS Recuperación de desastres

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateFailbackClientToRecoveryInstanceForDrs [solo permiso]	Concede permiso para obtener el cliente de conmutación por recuperación asociado a la instancia de recuperación.	Escritura	RecoveryInstanceResource*		
AssociateSourceNetworkStack	Otorga permiso para asociar la CloudFormation pila a la red de origen	Escritura	SourceNetworkResource*		cloudformation:DescribeStackResource cloudformation:DescribeStacks drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunch

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					TemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchCreateVolumeSnapshotGroupForDrs [solo permiso]	Concede permiso para crear grupo de instantáneas de volumen de lote.	Escritura	RecoveryInstanceResource*		
			SourceServerResource*		
BatchDeleteSnapshotRequestForDrs [solo permiso]	Concede permiso para eliminar la solicitud de instantáneas por lotes	Escritura			
CreateConvertedSnapshotForDrs [solo permiso]	Concede permiso para crear una instantánea convertida	Escritura	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtendedSourceServer	Concede permiso para extender un servidor de origen	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	drs:DescribeSourceServers drs:GetReplicationConfiguration

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLaunchConfigurationTemplate	Concede permiso para lanzar una plantilla de configuración de lanzamiento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryInstanceForDrs [solo permiso]	Concede permiso para crear una instancia de recuperación.	Escritura	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateReplicationConfigurationTemplate	Concede permiso para crear la plantilla de configuración de reproducción	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey
CreateSourceNetwork	Concede permiso para crear una red de origen	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSourceServerForDrs [solo permiso]	Concede permiso para crear un servidor de origen.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJob	Concede permiso para eliminar un trabajo.	Escritura	JobResource*		
DeleteLaunchAction	Otorga permiso para eliminar una acción de lanzamiento	Escritura	LaunchConfigurationTemplateResource		
			SourceServerResource		
DeleteLaunchConfigurationTemplate	Concede permiso para eliminar una plantilla de configuración de lanzamiento	Escritura	LaunchConfigurationTemplateResource*		
DeleteRecoveryInstance	Concede permiso para eliminar una instancia de recuperación.	Escritura	RecoveryInstanceResource*		
DeleteReplicationConfigurationTemplate	Concede permiso para eliminar la plantilla de configuración de reproducción	Escritura	ReplicationConfigurationTemplateResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSourceNetwork	Concede permiso para eliminar una red de origen	Escritura	SourceNetworkResource*		
DeleteSourceServer	Concede permiso para eliminar el servidor de origen	Write	SourceServerResource*		
DescribeJobLogItems	Concede permiso para describir elementos de registro de trabajo	Read	JobResource*		
DescribeJobs	Concede permiso para describir trabajos	Lectura			
DescribeLaunchConfigurationTemplates	Concede permiso para describir la plantilla de configuración de lanzamiento	Lectura			
DescribeRecoveryInstances	Concede permiso para describir instancias de recuperación.	Lectura			drs:DescribeSourceServers ec2:DescribeInstances
DescribeRecoverySnapshots	Concede permiso para describir instancias de recuperación.	Lectura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReplicationConfigurationTemplates	Concede permiso para describir la plantilla de configuración de reproducción	Lectura			
DescribeReplicationServerAssociationsForDrs [solo permiso]	Concede permiso para describir asociaciones de servidor de reproducción	Read			
DescribeSnapshotRequestsForDrs [solo permiso]	Concede permiso para describir solicitudes de instantáneas.	Lectura			
DescribeSourceNetworks	Concede permiso para describir redes de origen	Lectura			
DescribeSourceServers	Concede permiso para describir servidores de origen	Lectura			
DisconnectRecoveryInstance	Concede permiso para desconectar una instancia de recuperación.	Escritura	RecoveryInstanceResource*		
DisconnectSourceServer	Concede permiso para desconectar el servidor de origen.	Escritura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExportSourceNetworkCfnTemplate	Otorga permiso para exportar la CloudFormation plantilla que contiene los recursos de la red de origen	Escritura	SourceNetworkResource*		s3:GetBucketLocation s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAgentCommandForDrs [solo permiso]	Concede permiso para obtener el comando del agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentConfirmedResumeInfoForDrs [solo permiso]	Concede permiso para obtener información de reanudación confirmada del agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAgentInstallationAssetsForDrs [solo permiso]	Concede permiso para obtener activos de instalación del agente	Read			
GetAgentReplicationInfoForDrs [solo permiso]	Concede permiso para obtener información de reproducción del agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentRuntimeConfigurationForDrs [solo permiso]	Concede permiso para obtener la configuración de tiempo de ejecución del agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentSnapshotCreditsForDrs [solo permiso]	Concede permiso para obtener créditos de instantáneas del agente.	Lectura	RecoveryInstanceResource*		
			SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetChannelCommandsForDrs [solo permiso]	Concede permiso para obtener comandos de canal	Lectura			
GetFailbackCommandForDrs [solo permiso]	Concede permiso para obtener comandos de conmutación.	Lectura	RecoveryInstanceResource*		
GetFailbackLaunchRequestedForDrs [solo permiso]	Concede permiso para obtener el lanzamiento de conmutación por recuperación solicitado.	Lectura	RecoveryInstanceResource*		
GetFailbackReplicationConfiguration	Concede permiso para obtener la configuración de replicación de conmutación por recuperación.	Lectura	RecoveryInstanceResource*		
GetLaunchConfiguration	Concede permiso para obtener la configuración de lanzamiento	Read	SourceServerResource*		
GetReplicationConfiguration	Concede permiso para obtener la configuración de reproducción	Lectura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSuggestedFailbackClientDeviceMappingForDrs [solo permiso]	Concede permiso para obtener una asignación de dispositivos de cliente de conmutación por recuperación sugerida.	Lectura	RecoveryInstanceResource*		
InitializeService	Concede permiso para inicializar el servicio	Escritura			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueAgentCertificateForDrs [solo permiso]	Concede permiso para emitir un certificado de agente.	Escritura	RecoveryInstanceResource*		
			SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExtensibleSourceServers	Concede permiso para enumerar los servidores de origen extensibles	Lectura			drs:DescribeSourceServers
ListLaunchActions	Otorga permiso para enumerar acciones de lanzamiento	Lectura	LaunchConfigurationTemplateResource		
			SourceServerResource		
ListStagingAccounts	Concede permiso para enumerar las cuentas provisionales	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
NotifyAgentAuthenticationForDrs [solo permiso]	Concede permiso para notificar la autenticación del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentConnectedForDrs [solo permiso]	Concede permiso para notificar al agente conectado	Write	RecoveryInstanceResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			SourceServerResource*		
NotifyAgentDisconnectedForDrs [solo permiso]	Concede permiso para notificar al agente desconectado	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentReplicationProgressForDrs [solo permiso]	Concede permiso para notificar el progreso de reproducción del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyConsistencyAttainedForDrs [solo permiso]	Concede permiso para notificar la coherencia alcanzada.	Escritura	RecoveryInstanceResource*		
NotifyReplicationServerAuthenticationForDrs [solo permiso]	Concede permiso para notificar la autenticación del servidor de replicación.	Escritura	RecoveryInstanceResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
NotifyVolumeEventForDrs [solo permiso]	Concede permiso para notificar eventos de volumen del replicador.	Escritura	SourceServerResource*		
PutLaunchAction	Otorga permiso para realizar una acción de lanzamiento	Escritura	LaunchConfigurationTemplateResource		ssm:DescribeDocument
			SourceServerResource		
RetryDataReplication	Concede permiso para reintentar la replicación de datos.	Escritura	SourceServerResource*		
ReverseReplication	Otorga permiso para invertir la replicación	Escritura	RecoveryInstanceResource*		drs:DescribeReplicationConfigurationTemplates drs:DescribeSourceServers ec2:DescribeInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
SendAgentLogsForDrs [solo permiso]	Concede permiso para enviar registros del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
SendAgentMetricsForDrs [solo permiso]	Concede permiso para enviar métricas del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
SendChannelCommandResultForDrs [solo permiso]	Concede permiso para enviar el resultado del comando de canal	Write			
SendClientLogsForDrs [solo permiso]	Concede permiso para enviar registros de cliente	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendClientMetricsForDrs [solo permiso]	Concede permiso para enviar métricas de cliente	Escritura			
SendVolumeStatsForDrs [solo permiso]	Concede permiso para enviar estadísticas de rendimiento del volumen.	Escritura	SourceServerResource*		
StartFailbackLaunch	Concede permiso para iniciar el lanzamiento de la conmutación por recuperación.	Escritura	RecoveryInstanceResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartRecovery	Concede permiso para iniciar la recuperación.	Escritura	SourceServerResource*		drs:CreateRecoveryInstanceForDrs drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSnapshot

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:CreateTags ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StartReplication	Concede permiso para iniciar la replicación	Escritura	SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartSourceNetworkRecovery	Concede permiso para iniciar la recuperación de la red	Escritura	SourceNetworkResource*		cloudformation:CreateStack cloudformation:DescribeStackResource cloudformation:DescribeStacks cloudformation:UpdateStack drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunch

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					Templates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
StartSourceNetworkReplication	Concede permiso para iniciar la replicación de la red	Escritura	SourceNetworkResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopFailback	Concede permiso para detener la conmutación por recuperación.	Escritura	RecoveryInstanceResource*		
StopReplication	Concede permiso para detener la replicación	Escritura	SourceServerResource*		
StopSourceNetworkReplication	Concede permiso para detener la replicación de la red	Escritura	SourceNetworkResource*		
TagResource	Concede permiso para asignar una etiqueta de recurso.	Etiquetado	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			SourceServerResource		
				aws:RequestTag/${TagKey} aws:TagKeys drs:CreateAction	
Terminate RecoveryInstances	Concede permiso para terminar las instancias de recuperación.	Escritura	RecoveryInstanceResource*		drs:DescribeSourceServers ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateAgentBacklogForDrs [solo permiso]	Concede permiso para actualizar los pendientes del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentConversionInfoForDrs [solo permiso]	Concede permiso para actualizar la información de conversión del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationInfoForDrs [solo permiso]	Concede permiso para actualizar la información de reproducción del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationProcessStateForDrs [solo permiso]	Concede permiso para actualizar el estado del proceso de reproducción del agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAgentSourcePropertiesForDrs [solo permiso]	Concede permiso para actualizar las propiedades de origen del agente	Escritura	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateFailbackClientDeviceMappingForDrs [solo permiso]	Concede permiso para actualizar la asignación de dispositivos de cliente de conmutación por recuperación.	Escritura	RecoveryInstanceResource*		
UpdateFailbackClientLastSeenForDrs [solo permiso]	Concede permiso para actualizar el cliente de conmutación por recuperación visto por última vez.	Escritura	RecoveryInstanceResource*		
UpdateFailbackReplicationConfiguration	Concede permiso para actualizar la configuración de replicación.	Escritura	RecoveryInstanceResource*		
UpdateLaunchConfiguration	Concede permiso para actualizar la configuración de lanzamiento	Escritura	SourceServerResource*		ec2:DescribeInstances

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateLaunchConfigurationTemplate	Concede permiso para actualizar la configuración de lanzamiento	Escritura	LaunchConfigurationTemplateResource*		
UpdateReplicationCertificateForDrs [solo permiso]	Concede permiso para actualizar un certificado de replicación.	Escritura	RecoveryInstanceResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateReplicationConfiguration	Concede permiso para actualizar la configuración de reproducción	Write	SourceServerResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateReplicationConfigurationTemplate	Concede permiso para actualizar la plantilla de configuración de reproducción	Escritura	ReplicationConfigurationTemplateResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Tipos de recurso definidos por AWS Elastic Disaster Recovery

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
JobResource	`arn:${Partition}:drs:${Region}:${Account}:job/${JobID}`	aws:ResourceTag/${TagKey}
RecoveryInstanceResource	`arn:${Partition}:drs:${Region}:${Account}:recovery-instance/${RecoveryInstanceID}`	aws:ResourceTag/${TagKey} drs:EC2InstanceARN
ReplicationConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
SourceServerResource	`arn:${Partition}:drs:${Region}:${Account}:source-server/${SourceServerID}`	aws:ResourceTag/${TagKey}
SourceNetworkResource	`arn:${Partition}:drs:${Region}:${Account}:source-network/${SourceNetworkID}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery define las siguientes claves de condición que se pueden usar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
drs:CreateAction	Filtra el acceso mediante el nombre de una acción de API que crea recursos	Cadena
drs:EC2InstanceARN	Filtra el acceso por la EC2 instancia desde la que se originó la solicitud	ARN

Claves de condición, recursos y acciones de Amazon Elastic File System

Amazon Elastic File System (prefijo de servicio: `elasticfilesystem`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic File System
- Tipos de recursos definidos por Amazon Elastic File System
- Claves de condición de Amazon Elastic File System

Acciones definidas por Amazon Elastic File System

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Backup [solo permiso]	Concede permiso para iniciar un trabajo de copia de seguridad de un sistema de archivos existente	Write	file-system*		
ClientMount [solo permiso]	Concede permiso para que un cliente de NFS pueda tener acceso de lectura a un sistema de archivos	Read	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ClientRootAccess [solo permiso]	Concede permiso para que un cliente de NFS pueda tener acceso raíz a un sistema de archivos	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientWrite [solo permiso]	Concede permiso para que un cliente de NFS pueda tener acceso de escritura a un sistema de archivos	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	Concede permiso para crear un punto de acceso para el sistema de archivos especificado	Write	file-system*		elasticfilesystem:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFileSystem	Concede permiso para crear un nuevo sistema de archivos vacío	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource
CreateMountTarget	Concede permiso para crear un destino de montaje para un sistema de archivos	Escritura	file-system*		
CreateReplicationConfiguration	Concede permiso para crear una nueva configuración de replicación	Escritura	file-system*		
CreateTags	Otorga permiso para crear o sobrescribir las etiquetas asociadas a un sistema de archivos; en desuso, consulte TagResource	Etiquetado	file-system*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	Concede permiso para eliminar el punto de acceso especificado	Write	access-point*		
DeleteFileSystem	Concede permiso para eliminar un sistema de archivos, por lo que se corta permanentemente el acceso a su contenido	Write	file-system*		
DeleteFileSystemPolicy	Concede permiso para eliminar la política de nivel de recursos de un sistema de archivos	Administración de permisos	file-system*		
DeleteMountTarget	Concede permiso para eliminar el destino de montaje especificado	Escritura	file-system*		
DeleteReplicationConfiguration	Concede permiso para eliminar una configuración de replicación	Escritura	file-system*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTags	Concede permiso para eliminar las etiquetas especificadas de un sistema de archivos; en desuso, consulte UntagResource	Etiquetado	file-system*		
				aws:TagKeys	
DescribeAccessPoints	Concede permiso para ver las descripciones de los puntos de acceso de Amazon EFS	List	access-point		
			file-system		
DescribeAccountPreferences	Concede permiso para ver las preferencias de cuenta en vigor para una cuenta	Enumeración			
DescribeBackupPolicy	Otorga permiso para ver el BackupPolicy objeto para un sistema de archivos Amazon EFS	Lectura	file-system*		
DescribeFileSystemPolicy	Concede permiso para ver la política de nivel de recursos de un sistema de archivos de Amazon EFS	Lectura	file-system		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFileSystems	Otorga permiso para ver la descripción de un sistema de archivos Amazon EFS especificado por sistema de archivos FileSystemId; CreationToken o para ver la descripción de todos los sistemas de archivos propiedad de la persona que llama Cuenta de AWS en la AWS región del punto final al que se llama	Enumeración	file-system		
DescribeLifecycleConfiguration	Otorga permiso para ver el LifecycleConfiguration objeto para un sistema de archivos Amazon EFS	Lectura	file-system*		
DescribeMountTargetSecurityGroups	Concede permiso para ver los grupos de seguridad en vigor de un destino de montaje	Read	file-system*		
DescribeMountTargets	Concede permiso para ver las descripciones de todos los destinos de montaje o de un destino de montaje específico de un sistema de archivos	Lectura	file-system*		
			access-point		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReplicationConfigurations	Otorga permiso para ver la descripción de una configuración de replicación de Amazon EFS especificada por FileSystemId; o para ver la descripción de todas las configuraciones de replicación propiedad de la persona que llama Cuenta de AWS en la AWS región del punto final al que se llama	Enumeración	file-system		
DescribeTags	Concede permiso para ver las etiquetas asociadas a un sistema de archivos	Read	file-system*		
ListTagsForResource	Concede permiso para ver las etiquetas asociadas al recurso de Amazon EFS especificado	Read	access-point file-system		
ModifyMountTargetSecurityGroups	Concede permiso para modificar el conjunto de grupos de seguridad en vigor de un destino de montaje	Write	file-system*		
PutAccountPreferences	Concede permiso para establecer las preferencias de cuenta de una cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutBackupPolicy	Concede permiso para activar o desactivar las copias de seguridad automáticas con AWS Backup mediante la creación de un BackupPolicy objeto nuevo	Escritura	file-system*		
PutFileSystemPolicy	Concede permiso para aplicar una política de nivel de recursos que defina las acciones permitidas o denegadas de actores determinados para el sistema de archivos especificado	Administración de permisos	file-system*		
PutLifecycleConfiguration	Otorga permiso para habilitar la administración del ciclo de vida mediante la creación de un LifecycleConfiguration objeto nuevo	Escritura	file-system*		
ReplicationRead [solo permiso]	Otorga permiso para leer los datos del sistema de archivos para su replicación	Lectura	file-system*		
ReplicationWrite [solo permiso]	Otorga permiso para replicar datos en un sistema de archivos	Escritura	file-system*		
Restore [solo permiso]	Concede permiso para iniciar un trabajo de restauración de una copia de seguridad de un sistema de archivos	Write	file-system*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para crear o sobrescribir las etiquetas asociadas al recurso de Amazon EFS especificado	Etiquetado	access-point		
			file-system		
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	Concede permiso para eliminar las etiquetas especificadas de un recurso de Amazon EFS	Etiquetado	access-point		
			file-system		
				aws:TagKeys	
UpdateFileSystem	Concede permiso para actualizar el modo de rendimiento o la cantidad de rendimiento aprovisionado de un sistema de archivos existente.	Escritura	file-system*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFileSystemProtection	Concede permiso para actualizar la protección del sistema de archivos de un sistema de archivos existente	Escritura	file-system*		

Tipos de recursos definidos por Amazon Elastic File System

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
file-system	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
access-point	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Elastic File System

Amazon Elastic File System define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
elasticfilesystem:AccessPointArn	Filtra el acceso por el ARN del punto de acceso utilizado para montar el sistema de archivos	ARN
elasticfilesystem:AccessedViaMountTarget	Filtra el acceso según si se accede al sistema de archivos a través de destinos de montaje	Bool
elasticfilesystem:CreateAction	Filtra el acceso mediante el nombre de una acción de API que crea recursos	Cadena
elasticfilesystem:Encrypted	Filtra el acceso según si los usuarios solo pueden crear sistemas de archivos cifrados o no cifrados	Bool

Acciones, recursos y claves de condición para Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (prefijo de servicio: `eks`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic Kubernetes Service
- Tipos de recursos definidos por Amazon Elastic Kubernetes Service
- Claves de condición de Amazon Elastic Kubernetes Service

Acciones definidas por Amazon Elastic Kubernetes Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AccessKubernetesApi [solo permiso]	Otorga permiso para ver los objetos de Kubernetes a través de la consola EKS AWS	Lectura	cluster*		
AssociateAccessPolicy	Otorga permiso para asociar una política de acceso de Amazon EKS a una entrada de acceso de Amazon EKS	Escritura	access-entry*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				eks:policyArn eks:namespaces eks:accessScope	
AssociateEncryptionConfig	Concede permiso para asociar la configuración de cifrado a un clúster.	Write	cluster*		
AssociateIdentityProviderConfig	Concede permiso para asociar una configuración de proveedor de identidades a un clúster.	Escritura	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId eks:issuerUrl	
CreateAccessEntry	Concede permiso para crear una entrada de acceso de Amazon EKS	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Concede permiso para crear un complemento de Amazon EKS.	Write	cluster*		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCluster	Concede permiso para crear un clúster de Amazon EKS.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				eks:blockStorageEnabled	
CreateEksAnywhereSubscription	Concede permiso para crear una suscripción de EKS Anywhere	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Otorga permiso para crear un perfil de AWS Fargate	Escritura	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Concede permiso para crear un grupo de nodos de Amazon EKS.	Escritura	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	Concede permiso para crear una asociación EKS Pod Identity	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Concede permiso para eliminar una entrada de acceso de Amazon EKS	Escritura	access-entry*		
DeleteAddon	Concede permiso para eliminar un complemento de Amazon EKS.	Write	addon*		
			podidentityassociation		
DeleteCluster	Concede permiso para eliminar un clúster de Amazon EKS.	Escritura	cluster*		
DeleteEksAnywhereSubscription	Concede permiso para describir una suscripción a EKS Anywhere	Escritura	eks-anywhere-subscription*		
DeleteFargateProfile	Otorga permiso para eliminar un perfil de AWS Fargate	Escritura	fargateprofile*		
DeleteNodegroup	Concede permiso para eliminar un grupo de nodos de Amazon EKS.	Escritura	nodegroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePodIdentityAssociation	Concede permiso para eliminar una asociación de EKS Pod Identity	Escritura	podidentityassociation*		
DeregisterCluster	Concede permiso para anular el registro de un clúster externo	Escritura	cluster*		
DescribeAccessEntry	Concede permiso para describir una entrada de acceso de Amazon EKS	Lectura	access-entry*		
DescribeAddon	Concede permiso para recuperar información descriptiva sobre un complemento de Amazon EKS.	Lectura	addon*		
DescribeAddonConfiguration	Otorga permiso para enumerar opciones de configuración sobre un complemento de Amazon EKS	Lectura			
DescribeAddonVersions	Concede permiso para recuperar información descriptiva de la versión acerca de los complementos que son compatibles con los complementos de Amazon EKS.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCluster	Concede permiso para recuperar información descriptiva sobre un clúster de Amazon EKS.	Lectura	cluster*		
DescribeClusterVersions	Otorga permiso para recuperar información descriptiva sobre las versiones de Kubernetes que admiten los clústeres de Amazon EKS	Lectura			
DescribeEksAnywhereSubscription	Concede permiso para describir una suscripción a EKS Anywhere	Lectura	eks-anywhere-subscription*		
DescribeFargateProfile	Otorga permiso para recuperar información descriptiva sobre un perfil de AWS Fargate asociado a un clúster	Lectura	fargateprofile*		
DescribeIdentityProviderConfig	Concede permiso para recuperar información descriptiva sobre una configuración de ldp asociada a un clúster.	Lectura	identityproviderconfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInsight	Concede permiso para recuperar información descriptiva de una información detectada para un clúster especificado	Lectura	cluster*		
DescribeNodegroup	Concede permiso para recuperar información descriptiva sobre un grupo de nodos de Amazon EKS.	Lectura	nodegroup*		
DescribePodIdentityAssociation	Concede permisos para describir una asociación de EKS Pod Identity	Lectura	podidentityassociation*		
DescribeUpdate	Otorga permiso para recuperar una actualización determinada para un Amazon EKS cluster/nodegroup/add-on determinado (en la región especificada o predeterminada)	Lectura	cluster*		
			addon		
			nodegroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateAccessPolicy	Otorga permiso para desasociar una política de acceso de Amazon EKS de una entrada de acceso de Amazon EKS	Escritura	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
DisassociateIdentityProviderConfig	Concede permiso para eliminar una configuración de Idp asociada.	Escritura	identityproviderconfig*		
ListAccessEntries	Concede permiso para enumerar todas las entradas de acceso a Amazon EKS	Enumeración	cluster*		
ListAccessPolicies	Concede permiso para enumerar las políticas de acceso a Amazon EKS	Enumeración			
ListAddons	Otorga permiso para incluir los complementos de Amazon EKS en su región Cuenta de AWS (en la región especificada o predeterminada) para un clúster determinado	Enumeración	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssociatedAccessPolicies	Concede permisos para enumerar la política de acceso asociada y la entrada de acceso de Amazon EKS	Enumeración	access-entry*		
ListClusters	Otorga permiso para incluir los clústeres de Amazon EKS en su región Cuenta de AWS (en la región especificada o predeterminada)	Enumeración			
ListDashboardData	Otorga permiso para incluir los datos del panel de control. El panel de Amazon EKS agrega información sobre los recursos del clúster en varias cuentas y regiones. El panel incluye información sobre las EC2 instancias y las versiones del clúster EKS	Lectura	dashboard*		
ListDashboardResources	Otorga permiso para enumerar los recursos del panel de control. El panel de Amazon EKS agrega información sobre los recursos del clúster en varias cuentas y regiones. El panel incluye información sobre las EC2 instancias y las versiones del clúster EKS	Lectura	dashboard*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEksAnywhereSubscriptions	Concede permiso para enumerar suscripciones de EKS Anywhere	Enumeración			
ListFargateProfiles	Otorga permiso para incluir los perfiles de AWS Fargate en su región Cuenta de AWS (en la región especificada o predeterminada) asociados a un clúster determinado	Enumeración	cluster*		
ListIdentityProviderConfigs	Otorga permiso para enumerar las configuraciones de Idp asociadas a un clúster determinado Cuenta de AWS (en la región especificada o predeterminada)	Enumeración	cluster*		
ListInsights	Concede permisos para enumerar todos los conocimientos detectados para un clúster especificado	Enumeración	cluster*		
ListNodegroups	Otorga permiso para enumerar los grupos de nodos de Amazon EKS de su Cuenta de AWS clúster (en la región especificada o predeterminada) conectados a un clúster determinado	Enumeración	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPodIdentityAssociations	Concede permiso para enumerar asociaciones de EKS Pod Identity	Enumeración	cluster*		
ListTagsForResource	Concede permiso para enumerar las etiquetas del recurso especificado	Lectura	addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
ListUpdates	Otorga permiso para publicar las actualizaciones de un Amazon EKS cluster/nodegroup/add -on determinado (en la región especificada o predeterminada)	Enumeración	cluster*		
			addon		
			nodegroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterCluster	Concede permiso para registrar un clúster externo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para etiquetar el recurso especificado	Etiquetado	access-entry		
			addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para quitar las etiquetas del recurso especificado	Etiquetado	access-entry		
			addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateAccessEntry	Concede permiso para actualizar una entrada de acceso de Amazon EKS	Escritura	access-entry*		
UpdateAddon	Concede permiso para actualizar las configuraciones de los complementos de Amazon EKS, como la versión del VPC-CNI.	Write	addon*		
			podidentityassociation		
UpdateClusterConfig	Concede permiso para actualizar las configuraciones de clúster de Amazon EKS (p. ej.: acceso al punto de conexión del servidor de API).	Write	cluster*		
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateClusterVersion	Concede permiso para actualizar la versión de Kubernetes de un clúster de Amazon EKS.	Escritura	cluster*		
UpdateEksAnywhereSubscription	Concede permiso para actualizar una suscripción EKS Anywhere	Escritura	eks-anywhere-subscription*		
UpdateNodegroupConfig	Otorga permiso para actualizar las configuraciones de los grupos de nodos de Amazon EKS (p. ej., min/max/desired capacidad o etiquetas)	Escritura	nodegroup*		
UpdateNodegroupVersion	Concede permiso para actualizar la versión de Kubernetes de un grupo de nodos de Amazon EKS.	Escritura	nodegroup*		
UpdatePodIdentityAssociation	Concede permiso para actualizar una asociación de EKS Pod Identity	Escritura	podidentityassociation*		

Tipos de recursos definidos por Amazon Elastic Kubernetes Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
nodegroup	arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}	aws:ResourceTag/${TagKey}
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${ClusterName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	aws:ResourceTag/${TagKey}
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType

Tipos de recurso	ARN	Claves de condición
		eks:clusterName eks:kubernetesGroups eks:principalArn eks:username
access-policy	`arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}`	
dashboard	`arn:${Partition}:eks:${Region}:${Account}:dashboard/${DashboardName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por una clave que está presente en la solicitud que el usuario realiza al servicio EKS.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por la lista de todos los nombres de clave de etiqueta presentes en la solicitud que el usuario realiza al servicio EKS.	ArrayOfString
eks:accessEntryType	Filtra el acceso por el tipo de entrada de acceso presente en las solicitudes de entrada de acceso que el usuario realiza al servicio EKS	Cadena
eks:accessScope	Filtra el acceso por el accessScope presente en la política de acceso para asociar o desasociar que el usuario realiza al servicio EKS	Cadena
eks:authenticationMode	Filtra el acceso por el authenticationMode presente en la solicitud de creación o actualización del clúster	Cadena
eks:blockStorageEnabled	Filtra el acceso mediante el parámetro de almacenamiento en bloques habilitado en la solicitud de creación/actualización del clúster	Bool
eks:bootstrapClusterCreatorAdminPermissions	Filtra el acceso por el bootstrapClusterCreator AdminPermissions momento presente en la solicitud de creación de clúster	Bool
eks:bootstrapSelfManagedAddons	Filtra el acceso de los bootstrapSelfManaged complementos presentes en la solicitud de creación de clúster	Bool
eks:clientId	Filtra el acceso por el ClientiD presente en la solicitud de associateIdentityProvider Config que el usuario realiza al servicio EKS	Cadena
eks:clusterName	Filtra el acceso por el clusterName presente en las solicitudes de entrada de acceso que el usuario realiza al servicio EKS	Cadena

Claves de condición	Descripción	Tipo
eks:computeConfigEnabled	Filtra el acceso mediante el parámetro compute config enabled en la solicitud de creación/actualización del clúster	Bool
eks:elasticLoadBalancingEnabled	Filtra el acceso mediante el parámetro de equilibrio de carga elástico activado en la solicitud de creación o actualización del clúster	Bool
eks:issuerUrl	Filtra el acceso por la URL del emisor presente en la solicitud de associateIdentityProvider Config que el usuario realiza al servicio EKS	Cadena
eks:kubernetesGroups	Filtra el acceso por el kubernetesGroups presente en las solicitudes de entrada de acceso que el usuario realiza al servicio EKS	ArrayOfString
eks:namespaces	Filtra el acceso por el namespaces presente en la política de acceso para asociar o desasociar que el usuario realiza al servicio EKS	ArrayOfString
eks:policyArn	Filtra el acceso por el policyArn presente en las solicitudes de entrada de acceso que el usuario realiza al servicio EKS	ARN
eks:principalArn	Filtra el acceso por el principalArn presente en las solicitudes de entrada de acceso que el usuario realiza al servicio EKS	ARN
eks:supportType	Filtra el acceso por el supportType presente en la solicitud de creación o actualización del clúster	Cadena
eks:username	Filtra el acceso por el nombre de usuario de Kubernetes presente en las solicitudes de entrada de acceso que el usuario realiza al servicio EKS	Cadena

Acciones, recursos y claves de condición para AWS Elastic Load Balancing

AWS Elastic Load Balancing (prefijo de servicio:`elasticloadbalancing`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Elastic Load Balancing
- Tipos de recursos definidos por AWS Elastic Load Balancing
- Claves de condición para AWS Elastic Load Balancing

Acciones definidas por AWS Elastic Load Balancing

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTags	Concede permiso para agregar las etiquetas especificadas al equilibrador de carga especificado. Cada equilibrador de carga puede tener un máximo de 10 etiquetas	Etiquetado	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Concede permiso para asociar uno o varios grupos de seguridad con su equilibrador de carga en una nube privada virtual (VPC).	Escritura	loadbalancer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	Concede permiso para agregar una o varias subredes al conjunto de subredes configuradas para el equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConfigureHealthCheck	Concede permiso para especificar la configuración de la comprobación de estado que se debe utilizar al evaluar el estado de las instancias de backend.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateAppCookieStickinessPolicy	Concede permiso para generar una política de persistencia con las vidas útiles de las sesiones persistentes que siguen a una cookie generada por una aplicación.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLBCookieStickinessPolicy	Concede permiso para generar una política de persistencia con las vidas útiles de las sesiones persistentes controladas por la vida útil del navegador (usuario-agente), o por un periodo de vencimiento especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLoadBalancer	Concede permiso para crear un balanceador de carga	Escritura	loadbalancer		elasticloadbalancing:AddTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme elasticloadbalancing:Listen	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				erProtocol	
CreateLoadBalancerListeners	Concede permiso para crear uno o varios agentes de escucha para el equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	Concede permiso para crear una política con los atributos especificados para el equilibrador de carga especificado.	Escritura	loadbalancer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	Concede permiso para eliminar el equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLoadBalancerListeners	Concede permiso para eliminar los agentes de escucha especificados del equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	Concede permiso para eliminar la política especificada del equilibrador de carga especificado. Esta política no debe estar habilitada para ningún agente de escucha.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterInstancesFromLoadBalancer	Concede permiso para anular el registro de las instancias especificadas del equilibrador de carga especificado.	Escritura	loadbalancer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	Concede permiso para describir el estado de las instancias especificadas con respecto al equilibrador de carga especificado.	Lectura			
DescribeLoadBalancerAttributes	Concede permiso para describir los atributos para el equilibrador de carga especificado.	Lectura			
DescribeLoadBalancerPolicies	Concede permiso para describir las políticas especificadas.	Lectura			
DescribeLoadBalancerPolicyTypes	Concede permiso para describir los tipos de política de los equilibradores de carga especificados.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeLoadBalancers	Concede permiso para describir los equilibradores de carga especificados. Si no se especifican balanceadores de carga, la llamada describe todos los balanceadores de carga.	Enumeración			
DescribeTags	Concede permiso para describir las etiquetas asociadas con los equilibradores de carga especificados.	Lectura			
DetachLoadBalancerFromSubnets	Concede permiso para eliminar las subredes especificadas del conjunto de subredes configuradas para el equilibrador de carga.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableAvailabilityZonesForLoadBalancer	Concede permiso para quitar las zonas de disponibilidad especificadas del conjunto de zonas de disponibilidad para el equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	Concede permiso para agregar las zonas de disponibilidad especificadas al conjunto de zonas de disponibilidad para el equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Concede permiso para modificar los atributos del equilibrador de carga especificado.	Escritura	loadbalancer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	Concede permiso para agregar las instancias especificadas al equilibrador de carga especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Concede permiso para eliminar una o más etiquetas del equilibrador de carga especificado.	Etiquetado	loadbalancer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerListenerSSLCertificate	Concede permiso para establecer el certificado que termina las conexiones SSL del agente de escucha especificado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetLoadBalancerPoliciesForBackendServer	Concede permiso para sustituir el conjunto de políticas asociadas al puerto especificado en el que el servidor de backend está escuchando con un nuevo conjunto de políticas.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesOfListener	Concede permiso para sustituir el conjunto de políticas que se aplican actualmente en el puerto del equilibrador de carga especificado por el conjunto de políticas proporcionado.	Escritura	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Tipos de recursos definidos por AWS Elastic Load Balancing

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Claves de condición para AWS Elastic Load Balancing

AWS Elastic Load Balancing define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
elasticloadbalancing:CreateAction	Filtra el acceso mediante el nombre de una acción de API que crea recursos	Cadena
elasticloadbalancing:ListenerProtocol	Filtra el acceso mediante los protocolos del oyente permitidos en la solicitud	ArrayOfString
elasticloadbalancing:ResourceTag/	Filtra el acceso por la cadena de prefacio para una clave de etiqueta y un par de valores adjuntados a un recurso	Cadena
elasticloadbalancing:ResourceTag/${TagKey}	Filtra el acceso por la cadena de prefacio para una clave de etiqueta y un par de valores adjuntados a un recurso	Cadena
elasticloadbalancing:Scheme	Filtra el acceso mediante el esquema de equilibrador de carga permitido en la solicitud	Cadena
elasticloadbalancing:SecurityGroup	Filtra el acceso por el grupo de seguridad IDs permitido en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
elasticloadbalancing:SecurityPolicy	Filtra el acceso por las políticas de seguridad SSL permitidas en la solicitud	ArrayOfString
elasticloadbalancing:Subnet	Filtra el acceso por la subred IDs permitida en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 (prefijo de servicio:`elasticloadbalancing`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Elastic Load Balancing V2
- Tipos de recurso definidos por AWS Elastic Load Balancing V2
- Claves de condición de AWS Elastic Load Balancing V2

Acciones definidas por AWS Elastic Load Balancing V2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddListenerCertificates	Concede permiso para agregar los certificados especificados al agente de escucha seguro especificado.	Escritura	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AddTags	Concede permiso para agregar las etiquetas especificadas al equilibrador de carga especificado. Cada equilibrador de carga puede tener un máximo de 10 etiquetas	Etiquetado	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTrustStoreRevocations	Concede permiso para agregar revocaciones a un almacén de confianza	Escritura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateListener	Concede permiso para crear un oyente para el equilibrador de carga de aplicación especificado.	Escritura	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
CreateLoadBalancer	Concede permiso para crear un balanceador de carga	Escritura	loadbalancer/app/		elasticloadbalancing:AddTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			loadbalancer/gwy/		
			loadbalancer/net/		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRule	Concede permiso para crear una regla para su uso con el agente de escucha especificado.	Escritura	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	Concede permiso para crear un grupo de destino.	Escritura	targetgroup*		elasticloadbalancing:AddTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	Concede permiso para crear un almacén de confianza	Escritura	truststore		elasticloadbalancing:AddTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	Concede permiso para eliminar el agente de escucha especificado.	Escritura	listener/app*		
			listener/gwy*		
			listener/net*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancer	Concede permiso para eliminar el equilibrador de carga especificado.	Escritura	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	Concede permiso para eliminar la regla especificada	Escritura	listener-rule/app*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteSharedTrustStoreAssociation	Concede permiso para eliminar la asociación de almacén de confianza compartido especificada	Escritura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTargetGroup	Concede permiso para eliminar el grupo de destino especificado.	Escritura	targetgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	Concede permiso para eliminar el almacén de confianza especificado	Escritura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	Concede permiso para anular el registro de los destinos especificados desde el grupo de destino especificado.	Escritura	targetgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	Otorga permiso para describir los límites de recursos de Elastic Load Balancing para el Cuenta de AWS	Lectura			
DescribeCapacityReservation	Otorga permiso para describir la reserva de capacidad de un balanceador de carga	Lectura			
DescribeListenerAttributes	Concede permiso para describir los atributos del agente de escucha especificado	Lectura			
DescribeListenerCertificates	Concede permiso para describir los certificados del agente de escucha seguro especificado.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeListeners	Concede permiso para describir los agentes de escucha especificados o los agentes de escucha para el equilibrador de carga de aplicación especificado.	Lectura			
DescribeLoadBalancerAttributes	Concede permiso para describir los atributos para el equilibrador de carga especificado.	Lectura			
DescribeLoadBalancers	Concede permiso para describir los equilibradores de carga especificados. Si no se especifican balanceadores de carga, la llamada describe todos los balanceadores de carga.	Lectura			
DescribeRules	Concede permiso para describir las reglas especificadas o las reglas del agente de escucha especificado.	Lectura			
DescribeSSLPolicies	Concede permiso para describir las políticas especificadas o todas las políticas que se utilizan para la negociación SSL.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeTags	Concede permiso para describir las etiquetas asociadas con el recurso especificado.	Lectura			
DescribeTargetGroupAttributes	Concede permiso para describir los atributos del grupo de destino especificado.	Lectura			
DescribeTargetGroups	Concede permiso para describir los grupos de destino especificados o todos sus grupos de destino.	Lectura			
DescribeTargetHealth	Concede permiso para describir el estado de los destinos especificados o todos sus destinos.	Lectura			
DescribeTrustStoreAssociations	Concede permiso para describir las asociaciones con un almacén de confianza	Lectura			
DescribeTrustStoreRevocations	Concede permiso para describir las revocaciones de los almacenes de confianza especificados o todas sus revocaciones relacionadas con un almacén de confianza	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeTrustStores	Concede permiso para describir los almacenes de confianza especificados o todos sus almacenes de confianza	Lectura			
GetResourcePolicy	Concede permiso para obtener la política de recursos asociada al recurso	Lectura	truststore		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreCaCertificatesBundle	Concede permiso para recuperar una agrupación de certificados de CA de un almacén de confianza	Lectura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTrustStoreRevocationContent	Concede permiso para recuperar el contenido de revocación de un almacén de confianza	Lectura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	Otorga permiso para modificar la reserva de capacidad de un balanceador de cargas	Escritura	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyIpPools	Otorga permiso para modificar los grupos de direcciones IP de un balanceador de cargas	Escritura	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	Concede permiso para modificar las propiedades especificadas del agente de escucha especificado.	Escritura	listener/app*		
			listener/gwy*		
			listener/net*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyListenerAttributes	Concede permiso para modificar los atributos del agente de escucha especificado	Escritura	listener/app*		
			listener/gwy*		
			listener/net*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Concede permiso para modificar los atributos del equilibrador de carga especificado.	Escritura	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyRule	Concede permiso para modificar la regla especificada.	Escritura	listener-rule/app*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	Concede permiso para modificar las comprobaciones que se utilizan al evaluar el estado de los destinos en el grupo de destino especificado.	Escritura	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroupAttributes	Concede permiso para modificar los atributos especificados del grupo de destino especificado.	Escritura	targetgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	Concede permiso para modificar el almacén de confianza especificado	Escritura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	Concede permiso para registrar los destinos especificados con el grupo de destino especificado.	Escritura	targetgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	Concede permiso para eliminar los certificados especificados del agente de escucha seguro especificado.	Escritura	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Concede permiso para eliminar una o más etiquetas del equilibrador de carga especificado.	Etiquetado	listener-rule/app		
			listener-rule/net		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	Concede permiso para eliminar revocaciones de un almacén de confianza	Escritura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetIpAddressType	Concede permiso para establecer el tipo de direcciones IP utilizadas por las subredes del equilibrador de carga especificado.	Escritura	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetRulePriorities	Concede permiso para establecer las prioridades de las reglas especificadas.	Escritura	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	Concede permiso para asociar los grupos de seguridad especificados con el equilibrador de carga especificado.	Escritura	loadbalancer/app/		
			loadbalancer/net/		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	Concede permiso para habilitar la zona de disponibilidad de las subredes especificadas para el equilibrador de carga especificado.	Escritura	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [solo permiso]	Otorga permiso para dar WebAcl permiso a WAF	Escritura			

Tipos de recurso definidos por AWS Elastic Load Balancing V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
listener/gwy	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/gwy/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
loadbalancer/gwy/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/gwy/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/net/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
targetgroup	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:targetgroup/${TargetGroupName}/${TargetGroupId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
truststore	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:truststore/${TrustStoreName}/${TrustStoreId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Claves de condición de AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
elasticloadbalancing:CreateAction	Filtra el acceso mediante el nombre de una acción de API que crea recursos	Cadena
elasticloadbalancing:ListenerProtocol	Filtra el acceso por el protocolo del oyente permitido en la solicitud	Cadena
elasticloadbalancing:ResourceTag/${TagKey}	Filtra el acceso por la cadena de prefacio para una clave de etiqueta y un par de valores adjuntados a un recurso	Cadena

Claves de condición	Descripción	Tipo
elasticloadbalancing:Scheme	Filtra el acceso por el esquema de equilibrador de carga permitido en la solicitud	Cadena
elasticloadbalancing:SecurityGroup	Filtra el acceso por el grupo de seguridad IDs permitido en la solicitud	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filtra el acceso por las políticas de seguridad SSL permitidas en la solicitud	ArrayOfString
elasticloadbalancing:Subnet	Filtra el acceso por la subred IDs permitida en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon Elastic MapReduce

Amazon Elastic MapReduce (prefijo de servicio:`elasticmapreduce`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic MapReduce
- Tipos de recursos definidos por Amazon Elastic MapReduce

- Claves de condición de Amazon Elastic MapReduce

Acciones definidas por Amazon Elastic MapReduce

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> La DescribeJobFlows API está obsoleta y, finalmente, se eliminará. Le recomendamos que utilice ListClusters, DescribeCluster ListSteps, ListInstanceGroups y ListBootstrapActions en su lugar

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AccessAllEventLogs	Otorga permiso para ver todos los registros de eventos en un servidor de historial de aplicaciones persistente	Escritura	cluster*		
AddInstanceFleet	Concede permiso para agregar una flota de instancias a un clúster en ejecución	Escritura	cluster*		
AddInstanceGroups	Concede permiso para agregar grupos de instancias a un clúster en ejecución	Escritura	cluster*		
AddJobFlowSteps	Concede permiso para agregar pasos nuevos a un clúster en ejecución	Escritura	cluster*		
				elasticmapreduce:ExecutionRoleArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTags	Concede permiso para agregar etiquetas a un recurso de Amazon EMR	Etiquetado	cluster		
			editor		
			notebook-execution		
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [solo permiso]	Concede permiso para adjuntar un bloc de notas de EMR a un motor de computación	Escritura	editor*		
CancelSteps	Concede permiso para cancelar un paso o pasos pendientes en un clúster en ejecución	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEditor [solo permiso]	Concede permiso para crear un bloc de notas de EMR	Escritura	cluster		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	Concede permiso para crear un servidor de historial de aplicaciones persistente	Escritura	cluster*		
CreateRepository [solo permiso]	Concede permiso para crear un repositorio de bloc de notas de EMR	Escritura			
CreateSecurityConfiguration	Concede permiso para crear una configuración de seguridad	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateStudio	Concede permiso para crear un EMR Studio	Escritura		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	Concede permiso para lanzar un EMR Studio mediante el modo de autenticación de IAM	Escritura	studio*		
CreateStudioSessionMapping	Concede permiso para crear una asignación de sesión de EMR Studio	Escritura	studio*		
DeleteEditor [solo permiso]	Concede permiso para eliminar una bloc de notas de EMR	Escritura	editor*		
DeleteRepository [solo permiso]	Concede permiso para eliminar un repositorio de bloc de notas de EMR	Escritura			
DeleteSecurityConfiguration	Concede permiso para eliminar una configuración de seguridad	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteStudio	Concede permiso para eliminar un EMR Studio	Escritura	studio*		
DeleteStudioSessionMapping	Concede permiso para eliminar una asignación de sesión de EMR Studio	Escritura	studio*		
DeleteWorkspaceAccess [solo permiso]	Concede permiso para impedir que una identidad abra un espacio de trabajo colaborativo	Administración de permisos	editor*		
DescribeCluster	Concede permiso para obtener detalles acerca de un clúster, incluido el estado, la configuración de hardware y de software, los ajustes de la VPC, etc.	Lectura	cluster*		
DescribeEditor [solo permiso]	Concede permiso para ver información sobre un bloc de notas, incluido el estado, el usuario, el rol, las etiquetas, la ubicación, etc.	Lectura	editor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeJobFlows	Concede permiso para describir detalles de los clústeres (flujos de trabajo). Esta API está obsoleta y terminará por eliminarse. Le recomendamos que utilice ListClusters, DescribeCluster ListSteps, ListInstanceGroups y ListBootstrapActions en su lugar	Lectura	cluster*		
DescribeNotebookExecution	Concede permiso para ver información sobre la ejecución de un bloc de notas	Lectura	notebook-execution*		
DescribePersistentAppUI	Concede permiso para describir un servidor de historial de aplicaciones persistente	Lectura	cluster*		
DescribeReleaseLabel	Concede permiso para ver información sobre una versión de EMR, como qué aplicaciones son compatibles	Lectura			
DescribeRepository [solo permiso]	Concede permiso para describir un repositorio de bloc de notas de EMR	Lectura			
DescribeSecurityConfiguration	Concede permiso para obtener detalles de una configuración de seguridad	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeStep	Concede permiso para obtener información sobre un paso de clúster	Lectura	cluster*		
DescribeStudio	Concede permiso para ver información sobre un EMR Studio	Lectura	studio*		
DetachEditor [solo permiso]	Concede permiso para desconectar un bloc de notas de EMR de un motor de computación	Escritura	editor*		
GetAutoTerminationPolicy	Concede permiso para recuperar la política de terminación automática asociada a un clúster	Lectura	cluster*		
GetBlockPublicAccessConfiguration	Otorga permiso para recuperar la configuración de acceso público del bloque EMR para la Cuenta de AWS región	Lectura			
GetClusterSessionCredentials	Concede permiso para recuperar las credenciales básicas HTTP asociadas a un rol de IAM de ejecución determinado para un clúster de EMR habilitado con control de acceso detallado	Escritura	cluster*		
				elasticmapreduce:ExecutionRoleArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetManagedScalingPolicy	Concede permiso para recuperar la política de escalado administrado asociada a un clúster	Lectura	cluster*		
GetOnClusterAppUIPresignedURL	Concede permiso para obtener una URL prefirmada para un servidor de historial de aplicaciones que se ejecuta en el clúster	Escritura	cluster*		
GetPersistentAppUIPresignedURL	Concede permiso para obtener una dirección URL prefirmada para un servidor de historial de aplicaciones persistente	Escritura	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	Concede permiso para ver información sobre una asignación de sesión de EMR Studio	Lectura	studio*		
LinkRepository [solo permiso]	Concede permiso para enlazar un repositorio de un bloc de notas de EMR a EMR Notebooks	Escritura			
ListBootstrapActions	Concede permiso para obtener información detallada sobre las acciones de arranque asociadas a un clúster	Lectura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListClusters	Concede permiso para obtener el estado de los clústeres accesibles	Enumeración			
ListEditors [solo permiso]	Concede permiso para crear una lista de información resumida para EMR Notebooks accesible	Enumeración			
ListInstanceFleets	Concede permiso para obtener detalles de flotas de instancias en un clúster	Lectura	cluster*		
ListInstanceGroups	Concede permiso para obtener detalles de grupos de instancias en un clúster	Lectura	cluster*		
ListInstances	Otorga permiso para obtener detalles sobre las EC2 instancias de Amazon de un clúster	Lectura	cluster*		
ListNotebookExecutions	Concede permiso para crear una lista de la información resumida para las ejecuciones de los blocs de notas	Enumeración			
ListReleaseLabels	Concede permiso para crear una lista y filtrar las versiones de EMR disponibles en la Región actual	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRepositories [solo permiso]	Concede permiso para crear una lista de los repositorios de bloc de notas EMR existentes	Enumeración			
ListSecurityConfigurations	Concede permiso para crear una lista de las configuraciones de seguridad disponibles en esta cuenta por nombre, junto con las fechas y los horarios de creación	Enumeración			
ListSteps	Concede permiso para crear una lista de pasos asociados con un clúster	Lectura	cluster*		
ListStudioSessionMappings	Concede permiso para crear una lista de la información resumida acerca de las asignaciones de sesiones de un EMR Studio	Enumeración			
ListStudios	Concede permiso para crear una lista de la información resumida sobre EMR Studio	Enumeración			
ListSupportedInstanceTypes	Otorga permiso para enumerar los tipos de EC2 instancias de Amazon compatibles con una versión de Amazon EMR	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorkspaceAccessIdentities [solo permiso]	Concede permiso para enumerar las identidades a las que se les concede acceso a un espacio de trabajo	Enumeración	editor*		
ModifyCluster	Concede permiso para cambiar la configuración del clúster, como el número de pasos que se pueden ejecutar simultáneamente para un clúster	Escritura	cluster*		
ModifyInstanceFleet	Concede permiso para cambiar las capacidades de Spot y en diferido de destino para una flota de instancias	Escritura	cluster*		
ModifyInstanceGroups	Otorga permiso para cambiar el número y la configuración de las EC2 instancias de un grupo de instancias	Escritura	cluster		
OpenEditorInConsole [solo permiso]	Concede permiso para lanzar el editor de bloc de notas Jupyter para un bloc de notas de EMR desde la consola	Escritura	editor* cluster		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutAutoScalingPolicy	Concede permiso para crear o actualizar una política de escalado automático para un grupo de instancias central o un grupo de instancias de tareas	Escritura	cluster*		
PutAutoTerminationPolicy	Concede permiso para crear o actualizar la política de terminación automática asociada a un clúster	Escritura	cluster*		
PutBlockPublicAccessConfiguration	Otorga permiso para crear o actualizar la configuración de acceso público del bloque EMR para la Cuenta de AWS región	Administración de permisos			
PutManagedScalingPolicy	Concede permiso para crear o actualizar la política de escalado administrada asociada a un clúster	Escritura	cluster*		
PutWorkspaceAccess [solo permiso]	Concede permiso para permitir que una identidad abra un espacio de trabajo colaborativo	Administración de permisos	editor*		
RemoveAutoScalingPolicy	Concede permiso para eliminar una política de escalado automático de un grupo de instancias	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveAutoTerminationPolicy	Concede permiso para eliminar la política terminación automática asociada a un clúster	Escritura	cluster*		
RemoveManagedScalingPolicy	Concede permiso para eliminar la política de escalado administrada asociada a un clúster	Escritura	cluster*		
RemoveTags	Concede permiso para eliminar etiquetas de un recurso de Amazon EMR	Etiquetado	cluster		
			editor		
			notebook-execution		
			studio		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RunJobFlow	Concede permiso para crear y lanzar un clúster (flujo de trabajo)	Escritura		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	Concede permiso para agregar y eliminar la terminación automática después de la ejecución de pasos para un clúster	Escritura	cluster*		
SetTerminationProtection	Concede permiso para agregar y eliminar la protección de terminación para un clúster	Escritura	cluster*		
SetUnhealthyNodeReplacement	Concede permiso para habilitar o desactivar la sustitución de nodos en mal estado para un clúster	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetVisibleToAllUsers	Otorga permiso para establecer si todos los usuarios de AWS Identity and Access Management (IAM) del grupo Cuenta de AWS pueden ver un clúster. Esta API está obsoleta y es posible que todos los usuarios de la cuenta puedan ver el clúster. Para restringir el acceso a los clústeres mediante una política de IAM, consulte AWS Identity and Access Management for Amazon EMR https://docs.aws.amazon.com/emr/ latest/ManagementGuide/emr (plan-access-iam- .html)	Escritura	cluster*		
StartEditor [solo permiso]	Concede permiso para iniciar un bloc de notas de EMR	Escritura	editor*		
			cluster		
StartNotebookExecution	Concede permiso para iniciar la ejecución de un bloc de notas de EMR	Escritura	cluster*		
			editor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [solo permiso]	Concede permiso para cerrar un bloc de notas de EMR	Escritura	editor*		
StopNotebookExecution	Concede permiso para detener la ejecución del bloc de notas	Escritura	notebook-execution*		
TerminateJobFlows	Concede permiso para terminar un clúster (flujo de trabajo)	Escritura	cluster*		
UnlinkRepository [solo permiso]	Concede permiso para enlazar un repositorio de bloc de notas de EMR desde EMR Notebooks	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEditor [solo permiso]	Concede permiso para actualizar un EMR Notebook	Escritura	editor*		
UpdateRepository [solo permiso]	Concede permiso para actualizar un repositorio de bloc de notas de EMR	Escritura			
UpdateStudio	Concede permiso para actualizar la información sobre un EMR Studio	Escritura	studio*		
UpdateStudioSessionMapping	Concede permiso para actualizar una asignación de sesión de EMR Studio	Escritura	studio*		
ViewEventsFromAllClustersInConsole [solo permiso]	Concede permiso para utilizar la consola de EMR para ver eventos de todos los clústeres	Enumeración			

Tipos de recursos definidos por Amazon Elastic MapReduce

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
editor	arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
notebook-execution	arn:${Partition}:elasticmapreduce:${Region}:${Account}:notebook-execution/${NotebookExecutionId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
studio	arn:${Partition}:elasticmapreduce:${Region}:${Account}:studio/${StudioId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}

Claves de condición de Amazon Elastic MapReduce

Amazon Elastic MapReduce define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso en función de si el par de etiqueta y valor se proporciona con la acción	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso en función de si se ha asociado el par de etiqueta y valor con un recurso de Amazon EMR	Cadena
aws:TagKeys	Filtra el acceso en función de si las claves de etiqueta se proporcionan con la acción independientemente del valor de la etiqueta	ArrayOfString
elasticmapreduce:ExecutionRoleArn	Filtra las acciones en función de si el ARN del rol de ejecución se proporciona con la acción	ARN
elasticmapreduce:RequestTag/${TagKey}	Filtra el acceso en función de si el par de etiqueta y valor se proporciona con la acción	Cadena
elasticmapreduce:ResourceTag/${TagKey}	Filtra el acceso en función de si se ha asociado el par de etiqueta y valor con un recurso de Amazon EMR	Cadena

Acciones, recursos y claves de condición de Amazon Elastic Transcoder

Amazon Elastic Transcoder (prefijo de servicio: `elastictranscoder`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic Transcoder
- Tipos de recurso definidos por Amazon Elastic Transcoder
- Claves de condición de Amazon Elastic Transcoder

Acciones definidas por Amazon Elastic Transcoder

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelJob	Cancela una tarea que Elastic Transcoder no ha empezado a procesar.	Escritura	job*		
CreateJob	Creación de un trabajo	Escritura	pipeline*		
			preset*		
CreatePipeline	Cree una canalización	Escritura			
CreatePreset	Crear un elemento preestablecido	Escritura			
DeletePipeline	Elimina una canalización.	Write	pipeline*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePreset	Elimina un elemento preestablecido.	Write	preset*		
ListJobsByPipeline	Obtiene una lista de las tareas que asignó a una canalización.	Enumeración	pipeline*		
ListJobsByStatus	Obtenga información sobre todos los trabajos asociados al actual Cuenta de AWS que tienen un estado específico	Enumeración			
ListPipelines	Obtenga una lista de las tuberías asociadas a la actual Cuenta de AWS	Enumeración			
ListPresets	Obtenga una lista de todos los ajustes preestablecidos asociados a la actual Cuenta de AWS	Enumeración			
ReadJob	Obtiene información detallada sobre una tarea.	Read	job*		
ReadPipeline	Obtiene información detallada sobre una canalización.	Lectura	pipeline*		
ReadPreset	Obtiene información detallada sobre un elemento preestablecido.	Lectura	preset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TestRole	Pruebe la configuración de una canalización para garantizar que Elastic Transcoder pueda crear y procesar tareas.	Write			
UpdatePipeline	Actualiza la configuración de una canalización.	Write	pipeline*		
UpdatePipelineNotifications	Actualiza solo notificaciones de Amazon Simple Notification Service (Amazon SNS) para una canalización.	Escritura	pipeline*		
UpdatePipelineStatus	Pausa o vuelve a activar una canalización, de modo que esta deje de procesar tareas o reinicie el procesamiento, o actualiza el estado de la canalización.	Escritura	pipeline*		

Tipos de recurso definidos por Amazon Elastic Transcoder

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
job	`arn:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Claves de condición de Amazon Elastic Transcoder

Elastic Transcoder no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones de Amazon Elastic VMware Service

Amazon Elastic VMware Service (prefijo de servicio:`evs`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Elastic VMware Service
- Tipos de recursos definidos por Amazon Elastic VMware Service
- Claves de condición de Amazon Elastic VMware Service

Acciones definidas por Amazon Elastic VMware Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironment	Concede permiso para crear un entorno Amazon EVS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentHost	Otorga permiso para añadir un host a un entorno Amazon EVS	Escritura	environment*		
DeleteEnvironment	Otorga permiso para eliminar un entorno Amazon EVS	Escritura	environment*		
DeleteEnvironmentHost	Otorga permiso para eliminar un host de un entorno de Amazon EVS	Escritura	environment*		
GetEnvironment	Concede permiso para obtener un entorno Amazon EVS	Lectura	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEnvironmentHosts	Concede permiso para recuperar una lista de hosts asociados a un entorno Amazon EVS	Enumeración	environment*		
ListEnvironmentVlans	Concede permiso para recuperar una lista del entorno Amazon EVS VLANs	Enumeración	environment*		
ListEnvironments	Otorga permiso para recuperar una lista de los entornos de Amazon EVS de una cuenta	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un ARN de recurso especificado	Lectura	environment		
TagResource	Otorga permiso para etiquetar un ARN de recurso especificado	Etiquetado	environment*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permisos para eliminar las etiquetas de un ARN de recurso especificado	Etiquetado	environment*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por Amazon Elastic VMware Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment	`arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentIdentifier}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Elastic VMware Service

Amazon Elastic VMware Service define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon ElastiCache

Amazon ElastiCache (prefijo de servicio:`elasticache`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon ElastiCache
- Tipos de recursos definidos por Amazon ElastiCache
- Claves de estado de Amazon ElastiCache

Acciones definidas por Amazon ElastiCache

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Al crear una ElastiCache política en IAM, debe utilizar el carácter comodín «*» en el bloque de recursos. Para obtener información sobre el uso de las siguientes acciones de ElastiCache API en una política de IAM, consulte ElastiCache Acciones e IAM en la Guía ElastiCache del usuario de Amazon.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTagsToResource	Otorga permiso para añadir etiquetas a un recurso ElastiCache	Etiquetado	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
AuthorizeCacheSecurityGroupIngress	Otorga permiso para autorizar un grupo EC2 de seguridad en un grupo ElastiCache de seguridad	Escritura	securitygroup*		ec2:AuthorizeSecurityGroupIngress
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchApplyUpdateAction	Otorga permiso para aplicar actualizaciones de ElastiCache servicio a conjuntos de clústeres y grupos de replicación	Escritura	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchStopUpdateAction	Otorga permiso para impedir que las actualizaciones del ElastiCache servicio se ejecuten en un conjunto de clústeres	Escritura	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CompleteMigration	Otorga permiso para completar una migración en línea de datos desde Redis alojado en Amazon EC2 a ElastiCache	Escritura	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	Otorga permiso para conectarse como un ElastiCache usuario específico a un grupo de ElastiCache replicación o a una caché ElastiCache sin servidor	Escritura	user*		
			replicationgroup		
			serverlesscache		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CopyServerlessCacheSnapshot	Concede permiso para realizar una copia de una instantánea de caché sin servidor existente	Escritura	serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	Concede permiso para realizar una copia de una instantánea existente	Write	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCacheCluster	Concede permiso para crear un clúster de caché	Write	parameter group*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticache:CacheParameterGroupName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			securitygroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	Concede permiso para crear un grupo de parámetros	Write	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	
CreateCacheSecurityGroup	Concede permiso para crear un grupo de seguridad de caché	Write	securitygroup*		elasticache:AddTagsToResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	Concede permiso para crear un grupo de subred de caché	Write	subnetgroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalReplicationGroup	Concede permiso para crear un grupo de reproducción global	Write	globalreplicationgroup*		
			replicationgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
CreateReplicationGroup	Concede permiso para crear un grupo de reproducción	Escritura	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject
			cluster		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:AutomaticFailov	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				erEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticache:CacheParameterGroupName	
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateServerlessCache	Concede permiso para crear una caché sin servidor	Escritura	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineType elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit	ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTags ec2:DescribeVpcEndpoints ec2:DescribeVpcs elasticache:AddTagsToResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticache:MinimumECPUPerSecond elasticache:MaximumECPUPerSecond	s3:GetObject
			serverlesscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServerlessCacheSnapshot	Concede permiso para crear una copia de una caché sin servidor en un momento específico	Escritura	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Concede permiso para crear una copia de todo un clúster de Redis en un momento específico	Escritura	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
			cluster		
			replicationgroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
CreateUser	Otorga permiso para crear un usuario para Redis. Se admiten los usuarios a partir de Redis 6.0	Escritura	user*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	
CreateUserGroup	Otorga permiso para crear un grupo de usuarios para Redis. Se admiten los grupos a partir de Redis 6.0	Escritura	user*		elasticache:AddTagsToResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
DecreaseNodeGroupsInGlobalReplicationGroup	Concede permiso para reducir la cantidad de grupos de nodos en grupos de reproducción globales	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DecreaseReplicaCount	Concede permiso para reducir la cantidad de réplicas en un grupo de reproducción de Redis (modo de clúster deshabilitado) o la cantidad de nodos de réplica en uno o más grupos de nodos (particiones) de un grupo de reproducción de Redis (modo de clúster habilitado)	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCacheCluster	Concede permiso para eliminar un clúster aprovisionado anteriormente	Write	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteCacheParameterGroup	Concede permiso para eliminar el grupo de parámetros de caché especificado	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCacheSecurityGroup	Concede permiso para eliminar un grupo de seguridad de caché	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	
DeleteCacheSubnetGroup	Concede permiso para eliminar un grupo de subred de caché	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteGlobalReplicationGroup	Concede permiso para eliminar un grupo de reproducción global existente	Write	globalreplicationgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReplicationGroup	Concede permiso para eliminar un grupo de reproducción existente	Escritura	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	Concede permiso para eliminar una caché sin servidor	Escritura	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		
DeleteServerlessCacheSnapshot	Concede permiso para eliminar una instantánea de caché sin servidor	Escritura	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSnapshot	Concede permiso para eliminar una instantánea existente	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	Concede permiso para eliminar un usuario existente y, por lo tanto, eliminarlo de todos los grupos de usuarios y de reproducción donde se lo asignó	Write	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	Concede permiso para eliminar un grupo de usuarios existente	Write	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	Concede permiso para mostrar información sobre clústeres de caché aprovisionados	Enumeración	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeCacheEngineVersions	Concede permiso para crear una lista de los motores de caché disponibles y sus versiones	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCacheParameterGroups	Concede permiso para mostrar descripciones de grupos de parámetros de caché	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheParameters	Concede permiso para recuperar la lista de parámetros detallada de un grupo de parámetros de caché determinado	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	Concede permiso para mostrar descripciones de grupos de seguridad de caché	List	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	Concede permiso para mostrar descripciones de grupos de subred de caché	List	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeEngineDefaultParameters	Concede permiso para recuperar información predeterminada del motor y el parámetro del sistema para el motor de caché especificado	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEvents	Concede permiso para mostrar eventos relacionados con clústeres, grupos de seguridad de caché y grupos de parámetros de caché	List			
DescribeGlobalReplicationGroups	Concede permiso para mostrar información sobre grupos de reproducción globales	List	globalreplicationgroup*		
DescribeReplicationGroups	Concede permiso para mostrar información sobre grupos de reproducción aprovisionados	List	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	Concede permiso para mostrar información sobre los nodos de caché reservados adquiridos	List	reserved-instance*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodesOfferings	Concede permiso para mostrar ofertas de nodos de caché reservados disponibles	Enumeración			
DescribeServerlessCacheSnapshots	Concede permiso para enumerar información sobre las instantáneas de caché sin servidor	Enumeración	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	Concede permiso para enumerar cachés sin servidor	Enumeración	serverlesscache*	aws:ResourceTag/${TagKey}	
DescribeServiceUpdates	Concede permiso para mostrar los detalles de las actualizaciones del servicio	List			
DescribeSnapshots	Concede permiso para mostrar información sobre instantáneas de grupos de reproducción o clúster	List	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	Concede permiso para mostrar detalles de las acciones de actualización de un conjunto de clústeres o grupos de reproducción	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
DescribeUserGroups	Concede permiso para mostrar información sobre grupos de usuarios de Redis	List	usergroup*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeUsers	Concede permiso para mostrar información sobre usuarios de Redis	List	user*		
				aws:ResourceTag/${TagKey}	
DisassociateGlobalReplicationGroup	Concede permiso para quitar un grupo de reproducción secundario del grupo de reproducción global	Escritura	globalreplicationgroup*		
ExportServerlessCacheSnapshot	Concede permiso para exportar una copia de una caché sin servidor en un momento específico a un bucket S3	Escritura	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject
FailoverGlobalReplicationGroup	Concede permiso para conmutar por error la región principal a una región secundaria seleccionada de un grupo de reproducción global	Write	globalreplicationgroup*		
IncreaseNodeGroupsInGlobalReplicationGroup	Concede permiso para aumentar la cantidad de grupos de nodos en un grupo de reproducción global	Write	globalreplicationgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticache:NumNodeGroups	
IncreaseReplicaCount	Concede permiso para aumentar la cantidad de réplicas en un grupo de reproducción de Redis (modo de clúster deshabilitado) o la cantidad de nodos de réplica en uno o más grupos de nodos (particiones) de un grupo de reproducción de Redis (modo de clúster habilitado)	Escritura	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InterruptClusterAzPower [solo permiso]	Otorga permiso para probar una interrupción de alimentación en una zona de disponibilidad para un recurso ElastiCache	Escritura	replicationgroup*		
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeModifications	Concede permiso para mostrar el tipo de nodo disponible que se puede utilizar a fin de escalar un clúster de Redis o grupo de reproducción concreto	Enumeración	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un ElastiCache recurso	Lectura	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyCacheCluster	Concede permiso para modificar la configuración de un clúster	Write	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parametergroup		
			securitygroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	Concede permiso para modificar parámetros de un grupo de parámetros de caché	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	Concede permiso para modificar un grupo de subred de caché existente	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	Concede permiso para modificar la configuración de un grupo de reproducción global	Write	globalreplicationgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyReplicationGroup	Concede permiso para modificar la configuración de un grupo de reproducción	Write	replicationgroup*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName elasticache:Transi	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				tEncryptionEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyReplicationGroupShardConfiguration	Concede permiso para agregar y quitar particiones o volver a balancear los espacios clave entre particiones existentes de un grupo de reproducción	Escritura	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyServerlessCache	Concede permiso para modificar los parámetros para un caché sin servidor	Escritura	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MinimumECPUPerSecond elasticache:Maximu	ec2:DescribeSecurityGroups ec2:DescribeTags

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				mECPUPerSecond	
			usergroup	aws:ResourceTag/${TagKey}	
ModifyUser	Otorga permiso para cambiar la cadena de and/or acceso de las contraseñas de los usuarios de Redis	Escritura	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	Concede permiso para cambiar la lista de usuarios que pertenecen al grupo de usuarios	Write	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedCacheNodesOffering	Concede permiso para comprar una oferta de nodo de caché reservado	Write	reserved-instance*		elasticache:AddTagsToResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	Concede permiso para realizar una operación de rebalance o de espacio clave a fin de volver a distribuir ranuras y garantizar una distribución uniforme de claves entre particiones existentes en un grupo de reproducción global	Write	globalreplicationgroup*		
RebootCacheCluster	Concede permiso para reiniciar algunos o todos los nodos de caché dentro de un clúster de caché aprovisionado o grupo de reproducción (modo de clúster deshabilitado)	Escritura	cluster*		
				aws:ResourceTag/${TagKey}	
RemoveTagsFromResource	Otorga permiso para eliminar etiquetas de un recurso ElastiCache	Etiquetado	cluster		
			parametergroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResetCacheParameterGroup	Concede permiso para modificar los parámetros de un grupo de parámetros de caché a sus valores predeterminados	Escritura	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
RevokeCacheSecurityGroupIngress	Otorga permiso para eliminar la entrada EC2 de un grupo de seguridad de un grupo de ElastiCache seguridad	Escritura	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	Otorga permiso para iniciar una migración de datos de Redis alojado en Amazon EC2 a ElastiCache Redis	Escritura	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TestFailover	Concede permiso para probar la conmutación por error automática en un grupo de nodos especificado en un grupo de reproducción	Escritura	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
TestMigration	Otorga permiso para probar una migración de datos de Redis alojado en Amazon EC2 a ElastiCache Redis	Escritura	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon ElastiCache

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
parametergroup	`arn:${Partition}:elasticache:${Region}:${Account}:parametergroup:${CacheParameterGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName
securitygroup	`arn:${Partition}:elasticache:${Region}:${Account}:securitygroup:${CacheSecurityGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
subnetgroup	`arn:${Partition}:elasticache:${Region}:${Account}:subnetgroup:${CacheSubnetGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Tipos de recurso	ARN	Claves de condición
replicationgroup	`arn:${Partition}:elasticache:${Region}:${Account}:replicationgroup:${ReplicationGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled

Tipos de recurso	ARN	Claves de condición
		elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled

Tipos de recurso	ARN	Claves de condición
cluster	arn:${Partition}:elasticache:${Region}:${Account}:cluster:${CacheClusterId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AuthTokenEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:EngineType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:SnapshotRetentionLimit
reserved-instance	arn:${Partition}:elasticache:${Region}:${Account}:reserved-instance:${ReservedCacheNodeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Tipos de recurso	ARN	Claves de condición
snapshot	`arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Tipos de recurso	ARN	Claves de condición
globalreplicationgroup	`arn:${Partition}:elasticache::${Account}:globalreplicationgroup:${GlobalReplicationGroupId}`	elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit

Tipos de recurso	ARN	Claves de condición
		elasticache:TransitEncryptionEnabled
user	arn:${Partition}:elasticache:${Region}:${Account}:user:${UserId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode
usergroup	arn:${Partition}:elasticache:${Region}:${Account}:usergroup:${UserGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Tipos de recurso	ARN	Claves de condición
serverlesscache	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscache:${ServerlessCacheName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:DataStorageUnit elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MaximumDataStorage elasticache:MaximumECPUPerSecond elasticache:MinimumDataStorage elasticache:MinimumECPUPerSecond elasticache:SnapshotRetentionLimit

Tipos de recurso	ARN	Claves de condición
serverlesscachesnapshot	`arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Claves de estado de Amazon ElastiCache

Amazon ElastiCache define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

> **Note**
>
> Para construir elementos de condición mediante claves de condición de tipo cadena, utilice los operadores de condición que no distingan mayúsculas de minúsculas StringEqualsIgnoreCase o StringNotEqualsIgnoreCase compare una clave con un valor de cadena.
> Para obtener información sobre las condiciones de una política de IAM para controlar el acceso ElastiCache, consulte ElastiCache Keys in the Amazon ElastiCache User Guide.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso.	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se pasan en la solicitud	ArrayOfString
elasticache:AtRestEncryptionEnabled	Filtra el acceso por el AtRestEncryptionEnabled parámetro presente en la solicitud o por el valor predeterminado falso si el parámetro no está presente	Bool
elasticache:AuthTokenEnabled	Filtra el acceso por la presencia de un AuthToken parámetro que no esté vacío en la solicitud	Bool
elasticache:AutomaticFailoverEnabled	Filtra el acceso por el AutomaticFailoverEnabled parámetro de la solicitud	Bool
elasticache:CacheNodeType	Filtra el acceso por el cacheNodeType parámetro presente en la solicitud. Se puede utilizar esta clave para restringir qué tipos de nodo de caché se pueden utilizar en operaciones de creación o escalado de clústeres	Cadena
elasticache:CacheParameterGroupName	Filtra el acceso por el CacheParameterGroupName parámetro de la solicitud	Cadena

Claves de condición	Descripción	Tipo
elasticache:ClusterModeEnabled	Filtra el acceso por el parámetro de modo clúster presente en la solicitud. El valor predeterminado para las creaciones de un solo grupo de nodos (particiones) es falso	Bool
elasticache:DataStorageUnit	Filtra el acceso mediante CacheUsageLimits. DataStorageParámetro .Unit en la solicitud CreateServerlessCache and ModifyServerlessCache	Cadena
elasticache:EngineType	Filtra el acceso por el tipo de motor presente en las solicitudes de creación. En el caso de creaciones de grupos de replicación, el motor predeterminado “redis” se utiliza como clave si el parámetro no está presente	Cadena
elasticache:EngineVersion	Filtra el acceso por el parámetro engineVersion presente en las solicitudes de creación o modificación de clúster	Cadena
elasticache:KmsKeyId	Filtra el acceso por el identificador de clave de la clave KMS	Cadena
elasticache:MaximumDataStorage	Filtra el acceso por CacheUsageLimits. DataStorage.Parámetro máximo en la solicitud CreateServerlessCache and ModifyServerlessCache	Numérico
elasticache:MaximumECPUPerSecond	Filtra el acceso mediante. CacheUsageLimits ECPUPerSegundo. Parámetro máximo en la solicitud and CreateServerlessCache ModifyServerlessCache	Numérico
elasticache:MinimumDataStorage	Filtra el acceso mediante. CacheUsageLimits DataStorage.Parámetro mínimo en la solicitud CreateServerlessCache and ModifyServerlessCache	Numérico

Claves de condición	Descripción	Tipo
elasticache:MinimumECPUPerSecond	Filtra el acceso por. CacheUsageLimits ECPUPerSe gundo. Parámetro mínimo en la solicitud and CreateSer verlessCache ModifyServerlessCache	Numérico
elasticache:MultiAZEnabled	Filtra el acceso por AZMode parámetro, AZEnabled multiparámetro o número de zonas de disponibilidad en las que se puede ubicar el clúster o el grupo de replicaci ón	Bool
elasticache:NumNodeGroups	Filtra el acceso según el NodeGroupCount parámetro NumNodeGroups o especificado en la solicitud. Esta clave se puede utilizar para restringir la cantidad de grupos de nodos (particiones) que los clústeres pueden tener después de las operaciones de creación o escalado	Numérico
elasticache:ReplicasPerNodeGroup	Filtra el acceso por la cantidad de réplicas por grupo de nodos (particiones) especificados en creaciones o solicitudes de escalado	Numérico
elasticache:SnapshotRetentionLimit	Filtra el acceso por el SnapshotRetentionLimit parámetro de la solicitud	Numérico
elasticache:TransitEncryptionEnabled	Filtra el acceso por el TransitEncryptionEnabled parámetro presente en la solicitud. En el caso de creaciones de grupos de replicación, se utiliza el valor predeterminado ‘false’ como clave si el parámetro no está presente	Bool
elasticache:UserAuthenticationMode	Filtra el acceso por el UserAuthenticationMode parámetro de la solicitud	Cadena

Acciones, recursos y claves de condición para AWS Elemental Appliances and Software

AWS Elemental Appliances and Software (prefijo de servicio:`elemental-appliances-software`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Elemental Appliances and Software
- Tipos de recursos definidos por AWS Elemental Appliances and Software
- Claves de condición para AWS Elemental Appliances and Software

Acciones definidas por AWS Elemental Appliances and Software

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CompleteUpload [solo permiso]	Otorga permiso para completar la carga de un archivo adjunto a un presupuesto o pedido	Escritura			
CreateOrderV1 [solo permiso]	Concede permiso para crear un pedido	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateQuote [solo permiso]	Concede permiso para crear una cotización	Escritura	quote*		
GetAvsCorrectAddress [solo permiso]	Otorga permiso para validar una dirección	Lectura			
GetBillingAddresses [solo permiso]	Otorga permiso para incluir las direcciones de facturación en la AWS cuenta	Lectura			
GetDeliveryAddressesV2 [solo permiso]	Otorga permiso para incluir las direcciones de entrega en la AWS cuenta	Lectura			
GetOrder [solo permiso]	Otorga permiso para describir un pedido	Lectura			
GetOrdersV2 [solo permiso]	Otorga permiso para incluir los pedidos en la AWS cuenta	Lectura			
GetQuote [solo permiso]	Concede permiso para describir una cotización	Lectura	quote*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTaxes [solo permiso]	Otorga permiso para calcular los impuestos de un pedido	Lectura			
ListQuotes [solo permiso]	Otorga permiso para incluir las cotizaciones en la AWS cuenta	Enumeración			
StartUpload [solo permiso]	Otorga permiso para iniciar la carga de un archivo adjunto para un presupuesto o pedido	Escritura			
SubmitOrderV1 [solo permiso]	Otorga permiso para enviar un pedido	Escritura			
UpdateQuote [solo permiso]	Concede permiso para modificar una cotización	Escritura	quote*		

Tipos de recursos definidos por AWS Elemental Appliances and Software

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
quote	`arn:${Partition}:elemental-appliances-software:${Region}:${Account}:quote/${ResourceId}`	

Claves de condición para AWS Elemental Appliances and Software

Elemental Appliances and Software no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el servicio de activación de software y dispositivos de AWS Elemental

AWS El servicio de activación de dispositivos y software de Elemental (prefijo de servicio:`elemental-activations`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de activación de software y dispositivos de AWS Elemental
- Tipos de recursos definidos por el servicio de activación de software y dispositivos de AWS Elemental
- Claves de condición para el servicio de activación de software y dispositivos de AWS Elemental

Acciones definidas por el servicio de activación de software y dispositivos de AWS Elemental

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CompleteAccountRegistration [solo permiso]	Otorga permiso para completar el proceso de registro de la cuenta de cliente para las compras de dispositivos y software de AWS Elemental	Escritura			
CompleteFileUpload [solo permiso]	Otorga permiso para completar el proceso de carga de un archivo de software para las compras de software y electrodomésticos de AWS Elemental	Escritura			
ConfirmAccount [solo permiso]	Concede permiso para confirmar la propiedad de activos	Escritura			
DownloadKickstart [solo permiso]	Otorga permiso para descargar los archivos de inicio para las compras de dispositivos y software de AWS Elemental	Lectura			
DownloadSoftware [solo permiso]	Otorga permiso para descargar los archivos de software para las compras de software y electrodomésticos de AWS Elemental	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateLicense [solo permiso]	Otorga permiso para generar una licencia de software para la compra de dispositivos y software de AWS Elemental	Escritura			
GenerateLicenses [solo permiso]	Otorga permiso para generar licencias de software para la compra de dispositivos y software de AWS Elemental	Escritura			
GetArtifactGroupSoftwareVersions [solo permiso]	Concede permiso para describir la versión de software de un grupo de artefactos	Lectura			
GetAsset [solo permiso]	Concede permiso para describir un activo	Lectura			
GetAssets [solo permiso]	Concede permiso para describir los activos asociados a la cuenta que realiza la solicitud	Lectura			
GetProductAdvisories [solo permiso]	Concede permiso para obtener todos los avisos sobre productos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSoftwareVersions [solo permiso]	Concede permiso para describir las versiones de software disponibles	Lectura			
StartFileUpload [solo permiso]	Otorga permiso para iniciar el proceso de carga de un archivo de software para las compras de software y electrodomésticos de AWS Elemental	Escritura			

Tipos de recursos definidos por el servicio de activación de software y dispositivos de AWS Elemental

AWS El servicio de activación de software y dispositivos de Elemental no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al servicio de activación de software y dispositivos de AWS Elemental, especifique `"Resource": "*"` en la política.

Claves de condición para el servicio de activación de software y dispositivos de AWS Elemental

Elemental Activations no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de la política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de acción, recursos y condiciones de AWS Elemental MediaConnect

AWS Elemental MediaConnect (prefijo de servicio:`mediaconnect`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental AWS MediaConnect
- Tipos de recursos definidos por AWS Elemental MediaConnect
- Claves de condición de AWS Elemental MediaConnect

Acciones definidas por Elemental AWS MediaConnect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddBridgeOutputs	Otorga permiso para agregar salidas a un puente existente	Escritura	Bridge*		
AddBridgeSources	Otorga permiso para agregar orígenes a un puente existente	Escritura	Bridge*		
AddFlowMediaStreams	Otorga permiso para agregar secuencias multimedia a cualquier flujo.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddFlowOutputs	Otorga permiso para agregar salidas a cualquier flujo.	Write			
AddFlowSources	Otorga permiso para agregar orígenes a cualquier flujo.	Write			
AddFlowVpcInterfaces	Otorga permiso para agregar interfaces de VPC a cualquier flujo.	Escritura			
CreateBridge	Otorga permiso para crear puentes	Escritura	Bridge*		
CreateFlow	Otorga permiso para crear flujos.	Escritura			
CreateGateway	Otorga permiso para crear puertas de enlace	Escritura	Gateway*		
DeleteBridge	Otorga permiso para eliminar puentes	Escritura	Bridge*		
DeleteFlow	Otorga permiso para eliminar flujos.	Escritura			
DeleteGateway	Otorga permiso para eliminar puertas de enlace	Escritura	Gateway*		
DeregisterGatewayInstance	Otorga permiso para anular el registro de una instancia de puerta de enlace	Escritura	GatewayInstance*		
DescribeBridge	Otorga permiso para mostrar los detalles de un puente	Lectura	Bridge*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFlow	Otorga permiso para mostrar los detalles de un flujo, incluidos el ARN del flujo, su nombre y la zona de disponibilidad, así como detalles sobre el origen, las salidas y los derechos.	Lectura			
DescribeFlowSourceMetadata	Concede permiso para ver información sobre la secuencia de transporte de origen del flujo y los programas	Lectura			
DescribeFlowSourceThumbnail	Concede permiso para ver la miniatura de origen del flujo	Lectura			
DescribeGateway	Otorga permiso para mostrar los detalles de una puerta de enlace, incluidos el ARN, el nombre y los bloques CIDR de la pasarela, así como detalles sobre las redes	Lectura	Gateway*		
DescribeGatewayInstance	Otorga permiso para mostrar los detalles de una instancia de puerta de enlace	Lectura	GatewayInstance*		
DescribeOffering	Otorga permiso para mostrar los detalles de una oferta.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReservation	Otorga permiso para mostrar los detalles de una reserva.	Lectura			
DiscoverGatewayPollEndpoint	Otorga permiso para descubrir el punto de conexión final de sondeo de la puerta de enlace	Escritura			
GrantFlowEntitlements	Otorga permiso para otorgar derechos sobre cualquier flujo.	Escritura			
ListBridges	Otorga permiso para mostrar una lista de puentes asociados a esta cuenta y a un ARN especificado opcionalmente	Enumeración	Bridge*		
ListEntitlements	Otorga permiso para mostrar una lista de todos los derechos que se han otorgado a la cuenta.	List			
ListFlows	Otorga permiso para mostrar una lista de flujos asociados a esta cuenta.	Enumeración			
ListGatewayInstances	Otorga permiso para mostrar una lista de instancias asociadas a esta puerta de enlace	Enumeración	GatewayInstance*		
ListGateways	Otorga permiso para mostrar una lista de puertas de enlace asociadas a esta cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOfferings	Otorga permiso para mostrar una lista de todas las ofertas que están disponibles para la cuenta en la versión actual Región de AWS	Enumeración			
ListReservations	Otorga permiso para mostrar una lista de todas las reservas que la cuenta ha comprado en la cuenta actual Región de AWS	Enumeración			
ListTagsForResource	Otorga permiso para mostrar una lista de todas las etiquetas asociadas a un recurso.	Lectura			
PollGateway	Otorga permiso para sondear la puerta de enlace	Escritura			
PurchaseOffering	Otorga permiso para comprar una oferta.	Escritura			
RemoveBridgeOutput	Otorga permiso para eliminar una salida de un puente existente	Escritura	Bridge*		
RemoveBridgeSource	Otorga permiso para eliminar un origen de un puente existente	Escritura	Bridge*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveFlowMediaStream	Otorga permiso para eliminar secuencias multimedia de cualquier flujo.	Write			
RemoveFlowOutput	Otorga permiso para eliminar salidas de cualquier flujo.	Write			
RemoveFlowSource	Otorga permiso para eliminar orígenes de cualquier flujo.	Write			
RemoveFlowVpcInterface	Otorga permiso para eliminar interfaces VPC de cualquier flujo.	Write			
RevokeFlowEntitlement	Otorga permiso para revocar derechos sobre cualquier flujo.	Write			
StartFlow	Otorga permiso para comenzar flujos.	Write			
StopFlow	Otorga permiso para detener flujos.	Escritura			
SubmitGatewayStateChange	Otorga permiso para enviar el cambio de estado de la puerta de enlace	Escritura			
TagResource	Otorga permiso para asociar etiquetas a recursos.	Etiquetado			
UntagResource	Otorga permiso para eliminar etiquetas de recursos.	Etiquetado			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateBridge	Otorga permiso para actualizar puentes	Escritura	Bridge*		
UpdateBridgeOutput	Otorga permiso para actualizar una salida de un puente existente	Escritura	Bridge*		
UpdateBridgeSource	Otorga permiso para actualizar el origen de un puente existente	Escritura	Bridge*		
UpdateBridgeState	Otorga permiso para actualizar el estado de un puente existente	Escritura	Bridge*		
UpdateFlow	Otorga permiso para actualizar flujos.	Write			
UpdateFlowEntitlement	Otorga permiso para actualizar derechos sobre cualquier flujo.	Write			
UpdateFlowMediaStream	Otorga permiso para actualizar secuencias multimedia en cualquier flujo.	Write			
UpdateFlowOutput	Otorga permiso para actualizar salidas de cualquier flujo.	Write			
UpdateFlowSource	Otorga permiso para actualizar el origen de cualquier flujo.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGatewayInstance	Concede permiso para actualizar la configuración de una instancia de puerta de enlace existente	Escritura	GatewayInstance*		

Tipos de recursos definidos por AWS Elemental MediaConnect

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
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}`	

Tipos de recurso	ARN	Claves de condición
Gateway	`arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}`	
Bridge	`arn:${Partition}:mediaconnect:${Region}:${Account}:bridge:${FlowId}:${FlowName}`	
GatewayInstance	`arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}:instance:${InstanceId}`	

Claves de condición de AWS Elemental MediaConnect

MediaConnect no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de acción, recursos y condiciones de AWS Elemental MediaConvert

AWS Elemental MediaConvert (prefijo de servicio:`mediaconvert`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental AWS MediaConvert
- Tipos de recursos definidos por Elemental AWS MediaConvert
- Claves de condición de AWS Elemental MediaConvert

Acciones definidas por Elemental AWS MediaConvert

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate Certificate	Otorga permiso para asociar un Amazon Resource Name (ARN) de AWS Certificate Manager (ACM) a Elemental AWS MediaConvert	Escritura			
CancelJob	Otorga permiso para cancelar un MediaConvert trabajo de AWS Elemental que está en espera	Escritura	Job*		
CreateJob	Otorga permiso para crear y enviar un trabajo de AWS Elemental MediaConvert	Escritura	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				mediaconvert:HttpInputsAllowed mediaconvert:HttpsInputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Otorga permiso para crear una plantilla de trabajo MediaConvert personalizada de AWS Elemental	Escritura	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePreset	Otorga permiso para crear un ajuste preestablecido de salida MediaConvert personalizado de AWS Elemental	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateQueue	Otorga permiso para crear una cola de MediaConvert trabajos de AWS Elemental	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteJobTemplate	Otorga permiso para eliminar una plantilla de trabajo MediaConvert personalizada de AWS Elemental	Escritura	JobTemplate*		
DeletePolicy	Otorga permiso para eliminar una MediaConvert política de AWS Elemental	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePreset	Otorga permiso para eliminar un preset de salida MediaConvert personalizado de AWS Elemental	Escritura	Preset*		
DeleteQueue	Otorga permiso para eliminar una cola de MediaConvert trabajos de AWS Elemental	Escritura	Queue*		
DescribeEndpoints	Otorga permiso para suscribirse al MediaConvert servicio AWS Elemental mediante el envío de una solicitud para un punto de conexión específico de la cuenta. Todas las solicitudes de transcodificación deben enviarse al punto de enlace que el servicio devuelve	Enumeración			
DisassociateCertificate	Otorga permiso para eliminar una asociación entre el nombre de recurso de Amazon (ARN) de un AWS certificado de Certificate Manager (ACM) y un recurso de Elemental AWS MediaConvert	Escritura			
GetJob	Otorga permiso para obtener un AWS trabajo en Elemental MediaConvert	Lectura	Job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetJobTemplate	Otorga permiso para obtener una plantilla de MediaConvert trabajo de AWS Elemental	Lectura	JobTemplate*		
GetPolicy	Otorga permiso para obtener una MediaConvert política de AWS Elemental	Lectura			
GetPreset	Otorga permiso para obtener un ajuste preestablecido de MediaConvert salida de AWS Elemental	Lectura	Preset*		
GetQueue	Otorga permiso para obtener una lista de MediaConvert trabajos de AWS Elemental	Lectura	Queue*		
ListJobTemplates	Otorga permiso para publicar plantillas de MediaConvert trabajos de AWS Elemental	Enumeración			
ListJobs	Otorga permiso para publicar MediaConvert trabajos de AWS Elemental	Enumeración	Queue		
ListPresets	Otorga permiso para enumerar los ajustes AWS preestablecidos MediaConvert de salida de Elemental	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQueues	Otorga permiso para enumerar las colas de MediaConvert trabajos de AWS Elemental	Enumeración			
ListTagsForResource	Otorga permiso para recuperar las etiquetas de una lista, un MediaConvert ajuste preestablecido o una plantilla de trabajos	Lectura	Job		
			JobTemplate		
			Preset		
			Queue		
ListVersions	Otorga permiso para enumerar las versiones del motor de MediaConvert trabajo de AWS Elemental	Enumeración			
Probe	Otorga permiso para sondear un archivo	Lectura			
PutPolicy	Otorga permiso para poner una MediaConvert política de AWS Elemental	Escritura			
SearchJobs	Otorga permiso para buscar MediaConvert trabajos de AWS Elemental	Enumeración	Queue		
TagResource	Otorga permiso para añadir etiquetas a una MediaConvert lista, un ajuste preestablecido o una plantilla de trabajos	Etiquetado	Job		
			JobTemplate		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de una MediaConvert cola, un ajuste preestablecido o una plantilla de trabajos	Etiquetado	Job		
			JobTemplate		
			Preset		
			Queue		
				aws:TagKeys	
UpdateJobTemplate	Otorga permiso para actualizar una plantilla de trabajo MediaConvert personalizada de AWS Elemental	Escritura	JobTemplate*		
			Preset		
			Queue		
UpdatePreset	Otorga permiso para actualizar un ajuste preestablecido de salida MediaConvert personalizado de AWS Elemental	Escritura	Preset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQueue	Otorga permiso para actualizar una cola de MediaConvert trabajos de AWS Elemental	Escritura	Queue*		

Tipos de recursos definidos por Elemental AWS MediaConvert

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Job	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}`	aws:ResourceTag/${TagKey}
Queue	`arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}`	aws:ResourceTag/${TagKey}
Preset	`arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}`	aws:ResourceTag/${TagKey}
JobTemplate	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}`	aws:ResourceTag/${TagKey}
CertificateAssociation	`arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}`	

Claves de condición de AWS Elemental MediaConvert

AWS Elemental MediaConvert define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString
mediaconvert:HttpInputsAllowed	Filtra el acceso mediante una política de entrada HTTP presente en la cuenta	Bool
mediaconvert:HttpsInputsAllowed	Filtra el acceso mediante una política de entrada HTTPS presente en la cuenta	Bool
mediaconvert:S3InputsAllowed	Filtra el acceso mediante una política de entrada de S3 presente en la cuenta	Bool

Claves de acción, recursos y condiciones de AWS Elemental MediaLive

AWS Elemental MediaLive (prefijo de servicio:`medialive`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental AWS MediaLive
- Tipos de recursos definidos por Elemental AWS MediaLive
- Claves de condición de AWS Elemental MediaLive

Acciones definidas por Elemental AWS MediaLive

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptInputDeviceTransfer	Otorga permiso para aceptar la transferencia de un dispositivo de entrada.	Write	input-device*		
BatchDelete	Otorga permiso para eliminar canales, entradas, grupos de seguridad de entrada y multiplexores.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchStart	Otorga permiso para iniciar canales y multiplexores.	Write			
BatchStop	Otorga permiso para detener canales y multiplexores.	Write			
BatchUpdateSchedule	Otorga permiso para agregar y eliminar acciones de la programación de un canal.	Write	channel*		
CancelInputDeviceTransfer	Otorga permiso para cancelar la transferencia de un dispositivo de entrada.	Escritura	input-device*		
ClaimDevice	Otorga permiso para reclamar un dispositivo de entrada	Escritura	input-device*		
CreateChannel	Da permiso para crear un canal.	Escritura	channel*		
			input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelPlacementGroup	Concede permiso para crear un clúster	Escritura	channel-placement-group*		
			cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplate	Concede permiso para crear una plantilla de alarma de CloudWatch	Escritura	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplateGroup	Concede permiso para crear un grupo de plantillas de alarma de CloudWatch	Escritura	cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCluster	Concede permiso para crear un clúster	Escritura	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplate	Concede permiso para crear una plantilla de reglas de EventBridge	Escritura	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplateGroup	Concede permiso para crear un grupo de plantillas de reglas de EventBridge	Escritura	eventbridge-rule-template-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Da permiso para crear una entrada.	Write	input*		
			input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInputSecurityGroup	Da permiso para crear un grupo de seguridad de entrada.	Write	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplex	Otorga permiso para crear un multiplex	Write	multiplex*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplexProgram	Otorga permiso para crear un programa de multiplexor	Escritura	multiplex*		
CreateNetwork	Concede permiso para crear una red	Escritura	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNode	Concede permiso para crear un nodo	Escritura	cluster*		
			node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodeRegistrationScript	Concede permiso para crear un script de registro de nodos	Escritura	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePartnerInput	Otorga permiso para crear una entrada de socios	Escritura	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSdiSource	Otorga permiso para crear una fuente de SDI	Escritura	sdi-source*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalMap	Concede permiso para crear un mapa de señales	Escritura	signal-map*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTags	Otorga permiso para crear etiquetas para canales, entradas, grupos de seguridad de entrada, multiplexes, reservas, nodos, redes, clústeres, grupos de ubicación de canales, mapas de señales, fuentes SDI, grupos de plantillas y plantillas	Etiquetado	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Da permiso para eliminar un canal.	Escritura	channel*		
DeleteChannelPlacementGroup	Otorga permiso para eliminar un clúster	Escritura	channel-placement-group*		
DeleteCloudWatchAlarmTemplate	Concede permiso para eliminar una plantilla de alarma de CloudWatch	Escritura	cloudwatch-alarm-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCloudWatchAlarmTemplateGroup	Concede permiso para eliminar un grupo de plantillas de alarmas de CloudWatch	Escritura	cloudwatch-alarm-template-group*		
DeleteCluster	Otorga permiso para eliminar un clúster	Escritura	cluster*		
DeleteEventBridgeRuleTemplate	Concede permiso para eliminar una plantilla de regla de EventBridge	Escritura	eventbridge-rule-template*		
DeleteEventBridgeRuleTemplateGroup	Concede permiso para eliminar un grupo de plantillas de reglas de EventBridge	Escritura	eventbridge-rule-template-group*		
DeleteInput	Da permiso para eliminar una entrada.	Write	input*		
DeleteInputSecurityGroup	Da permiso para eliminar un grupo de seguridad de entrada.	Write	input-security-group*		
DeleteMultiplex	Otorga permiso para eliminar un multiplex	Write	multiplex*		
DeleteMultiplexProgram	Otorga permiso para eliminar un programa de multiplexor	Escritura	multiplex*		
DeleteNetwork	Concede permiso para eliminar una red	Escritura	network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteNode	Concede permiso para eliminar un nodo	Escritura	node*		
DeleteReservation	Da permiso para eliminar una reserva caducada.	Write	reservation*		
DeleteSchedule	Otorga permiso para eliminar todas las acciones de programación de un canal.	Escritura	channel*		
DeleteSdiSource	Otorga permiso para eliminar una fuente SDI	Escritura	sdi-source*		
DeleteSignalMap	Concede permiso para eliminar un mapa de señales	Escritura	signal-map*		
DeleteTags	Otorga permiso para eliminar etiquetas de canales, entradas, grupos de seguridad de entrada, multiplexes, reservas, nodos, clústeres, redes, grupos de ubicación de canales, fuentes SDI, mapas de señales, grupos de plantillas y plantillas	Etiquetado	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAccountConfiguration	Concede permiso para ver la configuración de cuenta del cliente	Lectura			
DescribeChannel	Da permiso para obtener detalles acerca de un canal.	Lectura	channel*		
DescribeChannelPlacementGroup	Concede permiso para describir un grupo de ubicación de canales	Lectura	channel-placement-group*		
DescribeCluster	Otorga permiso para describir un clúster	Lectura	cluster*		
DescribeInput	Da permiso para describir una entrada.	Read	input*		
DescribeInputDevice	Otorga permiso para describir un dispositivo de entrada	Read	input-device*		
DescribeInputDeviceThumbnail	Otorga permiso para describir una miniatura de dispositivo de entrada	Read	input-device*		
DescribeInputSecurityGroup	Da permiso para describir un grupo de seguridad de entrada.	Read	input-security-group*		
DescribeMultiplex	Otorga permiso para describir un multiplex	Read	multiplex*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMultiplexProgram	Otorga permiso para describir un programa de multiplexor	Lectura	multiplex*		
DescribeNetwork	Concede permiso para describir una red	Lectura	network*		
DescribeNode	Concede permiso para describir un nodo	Lectura	node*		
DescribeOffering	Da permiso para obtener información detallada acerca de una oferta de reserva.	Read	offering*		
DescribeReservation	Da permiso para obtener información detallada acerca de una reserva.	Read	reservation*		
DescribeSchedule	Otorga permiso para ver una lista de acciones programadas en un canal.	Lectura	channel*		
DescribeSdiSource	Otorga permiso para describir una fuente de SDI	Lectura	sdi-source*		
DescribeThumbnails	Concede permiso para ver las miniaturas de un canal	Lectura	channel*		
GetCloudWatchAlarmTemplate	Concede permiso para obtener una plantilla de alarma de CloudWatch	Lectura	cloudwatch-alarm-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCloudWatchAlarmTemplateGroup	Concede permiso para obtener un grupo de plantillas de alarmas de CloudWatch	Lectura	cloudwatch-alarm-template-group*		
GetEventBridgeRuleTemplate	Concede permiso para obtener una plantilla de regla de EventBridge	Lectura	eventbridge-rule-template*		
GetEventBridgeRuleTemplateGroup	Concede permiso para obtener un grupo de plantillas de reglas de EventBridge	Lectura	eventbridge-rule-template-group*		
GetSignalMap	Concede permiso para obtener un mapa de señales	Lectura	signal-map*		
ListChannelPlacementGroups	Concede permiso para enumerar grupos de ubicación de canales	Enumeración			
ListChannels	Da permiso para mostrar una lista de canales.	Enumeración			
ListCloudWatchAlarmTemplateGroups	Concede permiso para enumerar grupos de plantillas de alarmas de CloudWatch	Enumeración			
ListCloudWatchAlarmTemplates	Concede permiso para enumerar plantillas de alarmas de CloudWatch	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListClusters	Concede permiso para enumerar clústeres	Enumeración			
ListEventBridgeRuleTemplateGroups	Concede permiso para enumerar grupos de plantillas de reglas de EventBridge	Enumeración			
ListEventBridgeRuleTemplates	Concede permiso para enumerar plantillas de reglas de EventBridge	Enumeración			
ListInputDeviceTransfers	Otorga permiso para mostrar una lista de las transferencias de un dispositivo de entrada.	List			
ListInputDevices	Otorga permiso para mostrar una lista de dispositivos de entrada	List			
ListInputSecurityGroups	Da permiso para obtener una lista de grupos de seguridad de entrada.	List			
ListInputs	Da permiso para mostrar una lista de entradas.	List			
ListMultiplexPrograms	Otorga permisos para mostrar programas de multiplexor	List			
ListMultiplexes	Otorga permisos para mostrar multiplexes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNetworks	Concede permiso para enumerar redes	Enumeración			
ListNodes	Concede permiso para enumerar nodos	Enumeración			
ListOfferings	Da permiso para mostrar una lista de ofertas de reserva.	List			
ListReservations	Da permiso para mostrar una lista de reservas.	Enumeración			
ListSdiSources	Otorga permiso para incluir fuentes de SDI	Enumeración			
ListSignalMaps	Concede permiso para enumerar mapas de señales	Enumeración			
ListTagsForResource	Otorga permiso para enumerar etiquetas para canales, entradas, grupos de seguridad de entrada, multiplexes, reservas, nodos, clústeres, redes, grupos de ubicación de canales, fuentes SDI, mapas de señales, grupos de plantillas y plantillas	Enumeración	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListVersions	Otorga permiso para enumerar las versiones disponibles de MediaLive	Enumeración			
PollAnywhere	Concede permiso al nodo para sondear el clúster	Escritura			
PurchaseOffering	Da permiso para comprar una oferta de reserva.	Escritura	offering*		
			reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RebootInputDevice	Otorga permiso para reclamar un dispositivo de entrada	Escritura	input-device*		
RejectInputDeviceTransfer	Otorga permiso para rechazar la transferencia de un dispositivo de entrada.	Escritura	input-device*		
RestartChannelPipelines	Concede permiso para reiniciar canalizaciones en un canal en ejecución	Escritura	channel*		
StartChannel	Da permiso para comenzar un canal.	Escritura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDeleteMonitorDeployment	Concede permiso para iniciar la eliminación del monitor de un mapa de señales	Escritura	signal-map*		
StartInputDevice	Otorga permiso para iniciar un dispositivo de entrada conectado a un MediaConnect flujo	Escritura	input-device*		
StartInputDeviceMaintenanceWindow	Otorga permiso para iniciar un período de mantenimiento para un dispositivo de entrada	Escritura	input-device*		
StartMonitorDeployment	Concede permiso para iniciar la implementación de un monitor de mapa de señales	Escritura	signal-map*		
StartMultiplex	Otorga permisos para iniciar un multiplex	Escritura	multiplex*		
StartUpdateSignalMap	Concede permiso para iniciar una actualización del mapa de señales	Escritura	signal-map*		
StopChannel	Da permiso para detener un canal.	Escritura	channel*		
StopInputDevice	Otorga permiso para detener un dispositivo de entrada conectado a un MediaConnect flujo	Escritura	input-device*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopMultiplex	Otorga permiso para detener un multiplex	Escritura	multiplex*		
SubmitAnywhereStateChange	Concede permiso al nodo para enviar cambios de estado al clúster	Escritura			
TransferInputDevice	Otorga permiso para transferir un dispositivo de entrada.	Escritura	input-device*		
UpdateAccountConfiguration	Concede permiso para actualizar la configuración de cuenta del cliente	Escritura			
UpdateChannel	Da permiso para actualizar un canal.	Write	channel*		
UpdateChannelClass	Da permiso para actualizar la clase de un canal.	Escritura	channel*		
UpdateChannelPlacementGroup	Concede permiso para actualizar un nodo	Escritura	channel-placement-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCloudWatchAlarmTemplate	Concede permiso para actualizar una plantilla de alarma de CloudWatch	Escritura	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
UpdateCloudWatchAlarmTemplateGroup	Concede permiso para actualizar un grupo de plantillas de alarmas de CloudWatch	Escritura	cloudwatch-alarm-template-group*		
UpdateCluster	Otorga permiso para actualizar un clúster	Escritura	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEventBridgeRuleTemplate	Concede permiso para actualizar una plantilla de reglas de EventBridge	Escritura	eventbridge-rule-template*		
			eventbridge-rule-template-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEventBridgeRuleTemplateGroup	Concede permiso para actualizar un grupo de plantillas de reglas de EventBridge	Escritura	eventbridge-rule-template-group*		
UpdateInput	Da permiso para actualizar una entrada.	Write	input*		
UpdateInputDevice	Otorga permiso para actualizar un dispositivo de entrada	Write	input-device*		
UpdateInputSecurityGroup	Da permiso para actualizar un grupo de seguridad de entrada.	Write	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMultiplex	Otorga permiso para actualizar un multiplex	Write	multiplex*		
UpdateMultiplexProgram	Otorga permiso para actualizar un programa de multiplexor	Escritura	multiplex*		
UpdateNetwork	Concede permiso para actualizar el estado de un nodo	Escritura	network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNode	Concede permiso para actualizar un nodo	Escritura	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNodeState	Concede permiso para actualizar el estado de un nodo	Escritura	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateReservation	Da permiso para actualizar una reserva.	Escritura	reservation*		
UpdateSdiSource	Otorga permiso para actualizar el estado de una fuente de SDI	Escritura	sdi-source*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por Elemental AWS MediaLive

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
channel	`arn:${Partition}:medialive:${Region}:${Account}:channel:${ChannelId}`	aws:ResourceTag/${TagKey}
input	`arn:${Partition}:medialive:${Region}:${Account}:input:${InputId}`	aws:ResourceTag/${TagKey}
input-device	`arn:${Partition}:medialive:${Region}:${Account}:inputDevice:${DeviceId}`	
input-security-group	`arn:${Partition}:medialive:${Region}:${Account}:inputSecurityGroup:${InputSecurityGroupId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
multiplex	arn:${Partition}:medialive:${Region}:${Account}:multiplex:${MultiplexId}	aws:ResourceTag/${TagKey}
reservation	arn:${Partition}:medialive:${Region}:${Account}:reservation:${ReservationId}	aws:ResourceTag/${TagKey}
offering	arn:${Partition}:medialive:${Region}:${Account}:offering:${OfferingId}	
signal-map	arn:${Partition}:medialive:${Region}:${Account}:signal-map:${SignalMapId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template-group	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template-group:${CloudWatchAlarmTemplateGroupId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template:${CloudWatchAlarmTemplateId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template-group	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template-group:${EventBridgeRuleTemplateGroupId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template:${EventBridgeRuleTemplateId}	aws:ResourceTag/${TagKey}
cluster	arn:${Partition}:medialive:${Region}:${Account}:cluster:${ClusterId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
node	`arn:${Partition}:medialive:${Region}:${Account}:node:${ClusterId}/${NodeId}`	aws:ResourceTag/${TagKey}
network	`arn:${Partition}:medialive:${Region}:${Account}:network:${NetworkId}`	aws:ResourceTag/${TagKey}
channel-placement-group	`arn:${Partition}:medialive:${Region}:${Account}:channelPlacementGroup:${ClusterId}/${ChannelPlacementGroupId}`	aws:ResourceTag/${TagKey}
sdi-source	`arn:${Partition}:medialive:${Region}:${Account}:sdiSource:${SdiSourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Elemental MediaLive

AWS Elemental MediaLive define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de acción, recursos y condiciones de AWS Elemental MediaPackage

AWS Elemental MediaPackage (prefijo de servicio:`mediapackage`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental AWS MediaPackage
- Tipos de recursos definidos por AWS Elemental MediaPackage
- Claves de condición de AWS Elemental MediaPackage

Acciones definidas por Elemental AWS MediaPackage

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConfigureLogs	Otorga permiso para configurar registros de acceso para un Canal	Escritura	channels*		iam:CreateServiceLinkedRole
CreateChannel	Otorga permiso para crear un canal en Elemental AWS MediaPackage	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Otorga permiso para crear un trabajo de recolección en AWS Elemental MediaPackage	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Otorga permiso para crear un punto final en AWS Elemental MediaPackage	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Otorga permiso para eliminar un canal en AWS Elemental MediaPackage	Escritura	channels*		
DeleteOriginEndpoint	Otorga permiso para eliminar un punto final en AWS Elemental MediaPackage	Escritura	origin_endpoints*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeChannel	Otorga permiso para ver los detalles de un canal en AWS Elemental MediaPackage	Lectura	channels*		
DescribeHarvestJob	Otorga permiso para ver los detalles de un trabajo de recolección en AWS Elemental MediaPackage	Lectura	harvest_jobs*		
DescribeOriginEndpoint	Otorga permiso para ver los detalles de un punto final en AWS Elemental MediaPackage	Lectura	origin_endpoints*		
ListChannels	Otorga permiso para ver una lista de canales en AWS Elemental MediaPackage	Lectura			
ListHarvestJobs	Otorga permiso para ver una lista de trabajos de recolección en AWS Elemental MediaPackage	Lectura			
ListOriginEndpoints	Otorga permiso para ver una lista de puntos finales en Elemental AWS MediaPackage	Lectura			
ListTagsForResource	Otorga permiso para enumerar las etiquetas asignadas a un canal o OriginEndpoint	Lectura	channels		
			harvest_jobs		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			origin_endpoints		
RotateChannelCredentials	Otorga permiso para rotar las credenciales del primero IngestEndpoint de un canal en AWS Elemental MediaPackage	Escritura	channels*		
RotateIngestEndpointCredentials	Otorga permiso para rotar IngestEndpoint las credenciales de un canal en AWS Elemental MediaPackage	Escritura	channels*		
TagResource	Otorga permiso para etiquetar un MediaPackage recurso	Etiquetado	channels		
			harvest_jobs		
			origin_endpoints		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de un canal o OriginEndpoint	Etiquetado	channels		
			harvest_jobs		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			origin_endpoints		
				aws:TagKeys	
UpdateChannel	Otorga permiso para realizar cambios en un canal de AWS Elemental MediaPackage	Escritura	channels*		
UpdateOriginEndpoint	Otorga permiso para realizar cambios en un punto final de AWS Elemental MediaPackage	Escritura	origin_endpoints*		

Tipos de recursos definidos por AWS Elemental MediaPackage

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
channels	`arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
origin_endpoints	`arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}`	aws:ResourceTag/${TagKey}
harvest_jobs	`arn:${Partition}:mediapackage:${Region}:${Account}:harvest_jobs/${HarvestJobIdentifier}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Elemental MediaPackage

AWS Elemental MediaPackage define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la etiqueta de una MediaPackage solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por la etiqueta de un MediaPackage recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta de un MediaPackage recurso o solicitud	ArrayOfString

Claves de acciones, recursos y condiciones de AWS Elemental MediaPackage V2

AWS Elemental MediaPackage V2 (prefijo de servicio:`mediapackagev2`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental V2 AWS MediaPackage
- Tipos de recursos definidos por AWS Elemental MediaPackage V2
- Claves de condición de AWS Elemental MediaPackage V2

Acciones definidas por Elemental V2 AWS MediaPackage

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelHarvestJob	Otorga permiso para cancelar un trabajo de recolección	Escritura	Channel*		
			ChannelGroup*		
			HarvestJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			OriginEndpoint*		
CreateChannel	Concede permiso para crear un canal en un grupo de canales	Escritura	Channel*		
			ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelGroup	Concede permiso para crear un grupo de canales	Escritura	ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Otorga permiso para crear un trabajo de cosecha	Escritura	Channel*		
			ChannelGroup*		
			HarvestJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Concede permiso para crear un punto de conexión de origen para un canal	Escritura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Concede permiso para eliminar un canal de un grupo de canales	Escritura	Channel*		
			ChannelGroup*		
DeleteChannelGroup	Concede permiso para eliminar un grupo de canales	Escritura	ChannelGroup*		
DeleteChannelPolicy		Escritura	Channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para eliminar una política de recursos de un canal		ChannelGroup*		
			ChannelPolicy*		
DeleteOriginEndpoint	Concede permiso para eliminar un punto de conexión de origen de un canal	Escritura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
DeleteOriginEndpointPolicy	Concede permiso para eliminar una política de recursos de un punto de conexión de origen	Escritura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
GetChannel	Concede permiso para recuperar detalles de un canal de un grupo de canales	Lectura	Channel*		
			ChannelGroup*		
GetChannelGroup	Concede permiso para recuperar detalles de un grupo de canales	Lectura	ChannelGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetChannelPolicy	Concede permiso para recuperar una política de recursos para un canal	Lectura	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
GetHarvestJob	Otorga permiso para recuperar los detalles de un trabajo de cosecha	Lectura	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
GetHeadObject	Otorga permiso para realizar GetHeadObject solicitudes a MediaPackage	Lectura	OriginEndpoint*		
GetObject	Concede permiso para realizar GetObject solicitudes a MediaPackage	Lectura	OriginEndpoint*		
GetOriginEndpoint	Concede permiso para recuperar detalles de un punto de conexión de origen	Lectura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOriginEndpointPolicy	Concede permiso para recuperar detalles de una política de recursos para un punto de conexión de origen	Lectura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
HarvestObject	Concede permiso para realizar HarvestObject solicitudes a MediaPackage	Lectura	OriginEndpoint*		
ListChannelGroups	Concede permiso para enumerar todos los grupos de canales de una cuenta de AWS	Enumeración			
ListChannels	Concede permiso para enumerar todos los canales de un grupo de canales	Enumeración	ChannelGroup*		
ListHarvestJobs	Otorga permiso para enumerar todos los trabajos de recolección en un grupo de canales, un canal o un punto final de origen	Enumeración	ChannelGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOriginEndpoints	Concede permiso para enumerar todos los puntos de conexión de origen de un canal	Enumeración	Channel*		
			ChannelGroup*		
ListTagsForResource	Concede permiso para enumerar las etiquetas del recurso especificado	Lectura	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
PutChannelPolicy	Concede permiso para asociar una política de recursos para un canal	Escritura	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
PutObject	Otorga permiso para realizar PutObject solicitudes a MediaPackage	Escritura	Channel*		
PutOriginEndpointPolicy	Concede permiso para asociar una política de recursos a un punto de conexión de origen	Escritura	Channel*		
			ChannelGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			OriginEndpoint*		
			OriginEndpointPolicy*		
ResetChannelState	Otorga permiso para restablecer un canal	Escritura	Channel*		
			ChannelGroup*		
ResetOriginEndpointState	Otorga permiso para restablecer un punto final de origen	Escritura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
TagResource	Concede permiso para agregar las etiquetas especificadas al recurso especificado	Etiquetado	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para quitar las etiquetas especificadas de los recursos especificados	Etiquetado	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
				aws:TagKeys	
UpdateChannel	Concede permiso para actualizar un canal de un grupo de canales	Escritura	Channel*		
			ChannelGroup*		
UpdateChannelGroup	Concede permiso para actualizar un grupo de canales	Escritura	ChannelGroup*		
UpdateOriginEndpoint	Concede permiso para actualizar un punto de conexión de origen de un canal	Escritura	Channel*		
			ChannelGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			OriginEndpoint*		

Tipos de recursos definidos por AWS Elemental MediaPackage V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ChannelGroup	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}`	aws:ResourceTag/${TagKey}
ChannelPolicy	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	
Channel	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	aws:ResourceTag/${TagKey}
OriginEndpointPolicy	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	

Tipos de recurso	ARN	Claves de condición
OriginEndpoint	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	aws:ResourceTag/${TagKey}
HarvestJob	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}/harvestJob/${HarvestJobName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Elemental MediaPackage V2

AWS Elemental MediaPackage V2 define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de acciones, recursos y condiciones de AWS Elemental MediaPackage VOD

AWS El MediaPackage VOD elemental (prefijo de servicio:`mediapackage-vod`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental VOD AWS MediaPackage
- Tipos de recursos definidos por AWS Elemental MediaPackage VOD
- Claves de condición para AWS Elemental VOD MediaPackage

Acciones definidas por Elemental VOD AWS MediaPackage

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Configure Logs	Otorga permiso para configurar los registros de acceso de salida para un Packaging Group	Escritura	packaging-groups*		iam:CreateServiceLinkedRole
CreateAsset	Otorga permiso para crear un activo en Elemental AWS MediaPackage	Escritura		aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreatePackagingConfiguration	Otorga permiso para crear una configuración de empaquetado en AWS Elemental MediaPackage	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingGroup	Otorga permiso para crear un grupo de empaquetado en AWS Elemental MediaPackage	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Otorga permiso para eliminar un activo en AWS Elemental MediaPackage	Escritura	assets*		
DeletePackagingConfiguration	Otorga permiso para eliminar una configuración de empaquetado en AWS Elemental MediaPackage	Escritura	packaging-configurations*		
DeletePackagingGroup	Otorga permiso para eliminar un grupo de empaques en AWS Elemental MediaPackage	Escritura	packaging-groups*		
DescribeAsset	Otorga permiso para ver los detalles de un activo en AWS Elemental MediaPackage	Lectura	assets*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePackagingConfiguration	Otorga permiso para ver los detalles de una configuración de empaquetado en AWS Elemental MediaPackage	Lectura	packaging-configurations*		
DescribePackagingGroup	Otorga permiso para ver los detalles de un grupo de empaques en AWS Elemental MediaPackage	Lectura	packaging-groups*		
ListAssets	Otorga permiso para ver una lista de activos en AWS Elemental MediaPackage	Enumeración			
ListPackagingConfigurations	Otorga permiso para ver una lista de configuraciones de empaquetado en AWS Elemental MediaPackage	Enumeración			
ListPackagingGroups	Otorga permiso para ver una lista de grupos de empaques en AWS Elemental MediaPackage	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas asignadas a un Packaging Group PackagingConfiguration, o a un activo	Lectura	assets		
			packaging-configurations		
			packaging-groups		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para asignar etiquetas a un Packaging Group PackagingConfiguration, o a un activo	Etiquetado	assets		
			packaging-configurations		
			packaging-groups		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de un Packaging Group PackagingConfiguration, o un activo	Etiquetado	assets		
			packaging-configurations		
			packaging-groups		
				aws:TagKeys	
UpdatePackagingGroup	Otorga permiso para actualizar un grupo de empaques en AWS Elemental MediaPackage	Escritura	packaging-groups*		

Tipos de recursos definidos por AWS Elemental MediaPackage VOD

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
assets	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:assets/${AssetIdentifier}`	aws:ResourceTag/${TagKey}
packaging-configurations	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-configurations/${PackagingConfigurationIdentifier}`	aws:ResourceTag/${TagKey}
packaging-groups	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-groups/${PackagingGroupIdentifier}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Elemental VOD MediaPackage

AWS El MediaPackage VOD elemental define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Claves de acción, recursos y condiciones de AWS Elemental MediaStore

AWS Elemental MediaStore (prefijo de servicio:`mediastore`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental AWS MediaStore
- Tipos de recursos definidos por Elemental AWS MediaStore
- Claves de condición de AWS Elemental MediaStore

Acciones definidas por Elemental AWS MediaStore

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateContainer	Otorga permiso para crear un contenedor	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteContainer	Otorga permiso para eliminar un contenedor	Escritura	container*		
DeleteContainerPolicy	Otorga permiso para eliminar la política de acceso de un contenedor	Administración de permisos	container*		
DeleteCorsPolicy	Otorga permiso para eliminar la política de CORS de un contenedor	Escritura	container*		
DeleteLifecyclePolicy	Otorga permiso para eliminar la política de ciclo de vida de un contenedor	Escritura	container*		
DeleteMetricPolicy	Otorga permiso para eliminar la política de métricas de un contenedor	Escritura	container*		
DeleteObject	Otorga permiso para eliminar un objeto	Escritura	object*		
DescribeContainer	Otorga permiso para recuperar los detalles de un contenedor	Enumeración	container*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeObject	Otorga permiso para recuperar los metadatos de un objeto	Enumeración	object*		
GetContainerPolicy	Otorga permiso para recuperar la política de acceso de un contenedor	Lectura	container*		
GetCorsPolicy	Otorga permiso para recuperar la política de CORS de un contenedor	Lectura	container*		
GetLifecyclePolicy	Otorga permiso para recuperar la política de ciclo de vida que se asigna a un contenedor	Lectura	container*		
GetMetricPolicy	Otorga permiso para recuperar la política de métricas que se asigna a un contenedor	Lectura	container*		
GetObject	Otorga permiso para recuperar un objeto	Lectura	object*		
ListContainers	Otorga permiso para recuperar una lista de contenedores de la cuenta actual	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListItems	Otorga permiso para recuperar una lista de objetos y subcarpetas almacenados en una carpeta	Enumeración	folder		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un contenedor	Lectura	container		
PutContainerPolicy	Otorga permiso para crear o sustituir la política de acceso de un contenedor	Administración de permisos	container*		
PutCorsPolicy	Otorga permiso para agregar o modificar la política de CORS de un contenedor	Escritura	container*		
PutLifecyclePolicy	Otorga permiso para agregar o modificar la política de ciclo de vida que se asigna a un contenedor	Escritura	container*		
PutMetricPolicy	Otorga permiso para agregar o modificar la política de métricas que se asigna a un contenedor	Escritura	container*		
PutObject	Otorga permiso para cargar un objeto	Escritura	object*		
StartAccessLogging	Otorga permiso para iniciar sesión de acceso en un contenedor	Escritura	container*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopAccessLogging	Otorga permiso para detener sesión de acceso en un contenedor	Escritura	container*		
TagResource	Otorga permiso para agregar etiquetas a un contenedor	Etiquetado	container		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un contenedor	Etiquetado	container		
				aws:TagKeys	

Tipos de recursos definidos por Elemental AWS MediaStore

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
container	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}`	aws:ResourceTag/${TagKey}
object	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${ObjectPath}`	
folder	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${FolderPath}`	

Claves de condición de AWS Elemental MediaStore

AWS Elemental MediaStore define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de acción, recursos y condiciones de AWS Elemental MediaTailor

AWS Elemental MediaTailor (prefijo de servicio:`mediatailor`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Elemental AWS MediaTailor
- Tipos de recursos definidos por Elemental AWS MediaTailor
- Claves de condición de AWS Elemental MediaTailor

Acciones definidas por Elemental AWS MediaTailor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConfigureLogsForChannel	Otorga permiso para configurar los registros en el canal con el nombre de canal especificado	Escritura	channel*		
ConfigureLogsForPlaybackConfiguration	Otorga permiso para configurar registros para una configuración de reproducción	Escritura	playbackConfiguration*		iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateChannel	Otorga permiso para crear un canal un nuevo canal	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLiveSource	Otorga permiso para crear una nueva fuente activa en la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrefetchSchedule	Otorga permiso para crear una programación de recuperación previa para la configuración de reproducción con el nombre de configuración de reproducción especificado	Escritura	playbackConfiguration*		
CreateProgram	Otorga permiso para crear un nuevo programa en el canal con el nombre de canal especificado	Escritura			
CreateSourceLocation	Otorga permiso para crear una nueva ubicación de fuente	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVodSource	Otorga permiso para crear una nueva fuente de VOD en la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Otorga permisos para eliminar el canal con el nombre especificado	Escritura	channel*		
DeleteChannelPolicy	Otorga permiso para eliminar la política de IAM en el canal con el nombre de canal especificado	Administración de permisos	channel*		
DeleteLiveSource	Otorga permiso para eliminar la fuente activa con el nombre de fuente activa especificado en la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura	liveSource*		
DeletePlaybackConfiguration	Otorga permiso para eliminar la configuración de reproducción especificada	Escritura	playbackConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePrefetchSchedule	Otorga permiso para eliminar una programación de recuperación previa para una configuración de reproducción con el nombre de programación de recuperación previa especificado	Escritura	playbackConfiguration*		
			prefetchSchedule*		
DeleteProgram	Otorga permiso para eliminar el programa con el nombre de programa especificado en el canal con el nombre de canal especificado	Escritura	program*		
DeleteSourceLocation	Otorga permiso para eliminar la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura	sourceLocation*		
DeleteVodSource	Otorga permiso para eliminar la fuente de VOD con el nombre de fuente de VOD especificado en la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura	vodSource*		
DescribeChannel	Otorga permiso para recuperar el canal con el nombre de canal especificado	Lectura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeLiveSource	Otorga permiso para recuperar la fuente activa con el nombre de fuente activa especificado en la ubicación de fuente con el nombre de ubicación de fuente especificado	Lectura	liveSource*		
DescribeProgram	Otorga permiso para recuperar el programa con el nombre de programa especificado en el canal con el nombre de canal especificado	Lectura	program*		
DescribeSourceLocation	Otorga permiso para recuperar la ubicación de fuente con el nombre de ubicación de fuente especificado	Lectura	sourceLocation*		
DescribeVodSource	Otorga permiso para recuperar la fuente de VOD con el nombre de fuente de VOD especificado en la ubicación de fuente con el nombre de ubicación de fuente especificado	Lectura	vodSource*		
GetChannelPolicy	Otorga permiso para leer la política de IAM en el canal con el nombre de canal especificado	Lectura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetChannelSchedule	Otorga permiso para recuperar la programación de programas en el canal con el nombre de canal especificado	Lectura	channel*		
GetPlaybackConfiguration	Da permiso para recuperar la configuración del nombre especificado.	Lectura	playbackConfiguration*		
GetPrefetchSchedule	Otorga permiso para recuperar la programación de recuperación previa de una configuración de reproducción con el nombre de programación de recuperación previa especificado	Lectura	playbackConfiguration*		
			prefetchSchedule*		
ListAlerts	Otorga permiso para recuperar una lista de alertas de recursos	Lectura			
ListChannels	Otorga permiso para recuperar un canal de canales existente	Lectura			
ListLiveSources	Otorga permiso para recuperar la lista de fuentes activa existentes en la ubicación fuente con el nombre de ubicación de fuente especificado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPlaybackConfigurations	Da permiso para recuperar la lista de configuraciones disponibles.	Enumeración			
ListPrefetchSchedules	Otorga permiso para recuperar la lista de programaciones de recuperación previas para una configuración de reproducción	Enumeración	playbackConfiguration*		
ListSourceLocations	Otorga permiso para recuperar la lista de ubicaciones de fuente existentes	Lectura			
ListTagsForResource	Otorga permiso para listar las etiquetas asignadas al recurso de configuración de una reproducción especificada	Lectura	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
ListVodSources	Otorga permiso para recuperar la lista de fuentes VOD existentes en la ubicación fuente con el nombre de ubicación de fuente especificado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutChannelPolicy	Otorga permiso para establecer la política de IAM en el canal con el nombre de canal especificado	Administración de permisos	channel*		
PutPlaybackConfiguration	Da permiso para agregar una nueva configuración.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
StartChannel	Otorga permiso para iniciar el canal con el nombre de canal especificado	Escritura	channel*		
StopChannel	Otorga permiso para detener el canal con el nombre de canal especificado	Escritura	channel*		
TagResource	Otorga permiso para agregar las etiquetas al recurso de configuración de reproducción especificado	Etiquetado	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar las etiquetas del recurso de configuración de reproducción especificado	Etiquetado	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:TagKeys	
UpdateChannel	Otorga permiso para actualizar el canal con el nombre de canal especificado	Escritura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateLiveSource	Otorga permiso para actualizar la fuente activa con el nombre de fuente activa especificado en la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura	liveSource*		
UpdateProgram	Otorga permiso para actualizar el programa con el nombre de programa especificado en el canal con el nombre de canal especificado	Escritura	program*		
UpdateSourceLocation	Otorga permiso para actualizar la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura	sourceLocation*		
UpdateVodSource	Otorga permiso para actualizar la fuente de VOD con el nombre de fuente de VOD especificado en la ubicación de fuente con el nombre de ubicación de fuente especificado	Escritura	vodSource*		

Tipos de recursos definidos por Elemental AWS MediaTailor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
playbackConfiguration	`arn:${Partition}:mediatailor:${Region}:${Account}:playbackConfiguration/${ResourceId}`	aws:ResourceTag/${TagKey}
prefetchSchedule	`arn:${Partition}:mediatailor:${Region}:${Account}:prefetchSchedule/${ResourceId}`	
channel	`arn:${Partition}:mediatailor:${Region}:${Account}:channel/${ChannelName}`	aws:ResourceTag/${TagKey}
program	`arn:${Partition}:mediatailor:${Region}:${Account}:program/${ChannelName}/${ProgramName}`	
sourceLocation	`arn:${Partition}:mediatailor:${Region}:${Account}:sourceLocation/${SourceLocationName}`	aws:ResourceTag/${TagKey}
vodSource	`arn:${Partition}:mediatailor:${Region}:${Account}:vodSource/${SourceLocationName}/${VodSourceName}`	aws:ResourceTag/${TagKey}
liveSource	`arn:${Partition}:mediatailor:${Region}:${Account}:liveSource/${SourceLocationName}/${LiveSourceName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Elemental MediaTailor

AWS Elemental MediaTailor define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Elemental Support Cases

AWS Elemental Support Cases (prefijo de servicio:`elemental-support-cases`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Elemental Support Cases
- Tipos de recursos definidos por AWS Elemental Support Cases

- Claves de condición para AWS Elemental Support Cases

Acciones definidas por AWS Elemental Support Cases

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddCaseComment [solo permiso]	Otorga permiso para añadir un comentario a un caso de soporte	Escritura	case*		
CheckCasePermission [solo permiso]	Concede permiso para comprobar si la persona que llama tiene los permisos para realizar operaciones de casos de soporte	Escritura			
CompleteMultipartUpload [solo permiso]	Otorga permiso para completar la carga de un archivo de varias partes a un caso de soporte	Escritura	case*		
CreateCase [solo permiso]	Concede permiso para crear un caso de soporte	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateS3CLIUploadCommand	Otorga permiso para crear un comando cli que permita cargar un archivo en un caso de soporte	Escritura	case*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
[solo permiso]					
CreateS3DownloadUrl [solo permiso]	Otorga permiso para descargar un archivo de un caso de soporte	Escritura	case*		
GetCase [solo permiso]	Concede permiso para describir un caso de soporte en su cuenta	Lectura	case*		
GetCasePermission [solo permiso]	Concede permiso para comprobar si la persona que llama tiene los permisos para realizar operaciones de casos de soporte	Lectura			
GetCases [solo permiso]	Concede permiso para enumerar los casos de soporte de su cuenta	Lectura			
GetUICache [solo permiso]	Otorga permiso para recuperar los datos de usuario del caso almacenados en caché para utilizarlos en la consola	Lectura			
ListTagsForCase [solo permiso]	Otorga permiso para incluir etiquetas en un caso de soporte	Lectura	case*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartMultipartUpload [solo permiso]	Otorga permiso para iniciar la carga de un archivo de varias partes en un caso de soporte	Escritura	case*		
TagCase [solo permiso]	Otorga permiso para añadir una etiqueta a un caso de soporte	Etiquetado	case*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCase [solo permiso]	Otorga permiso para eliminar una etiqueta de un estuche de soporte	Etiquetado	case*		
				aws:TagKeys	
UpdateCase [solo permiso]	Concede permiso para actualizar un caso de soporte	Escritura	case*		
UpdateCaseStatus [solo permiso]	Otorga permiso para actualizar el estado de un caso de soporte	Escritura	case*		
UpdateMultipartUpload [solo permiso]	Otorga permiso para actualizar un archivo de varias partes subido a un caso de soporte	Escritura	case*		

Tipos de recursos definidos por AWS Elemental Support Cases

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
case	`arn:${Partition}:elemental-support-cases::${Account}:case/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Elemental Support Cases

AWS Elemental Support Cases define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Elemental Support Content

AWS Elemental Support Content (prefijo de servicio:`elemental-support-content`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Elemental Support Content
- Tipos de recursos definidos por AWS Elemental Support Content
- Claves de condición para AWS Elemental Support Content

Acciones definidas por AWS Elemental Support Content

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Query [solo permiso]	Concede permiso para buscar contenido de soporte	Lectura			

Tipos de recursos definidos por AWS Elemental Support Content

AWS El contenido de Elemental Support no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Elemental Support Content, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Elemental Support Content

Elemental Support Content no tiene claves de contexto específicas de servicio que se puedan utilizar en el elemento `Condition` de la instrucción de la política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon EMR on EKS (EMR Containers)

Amazon EMR on EKS (EMR Containers) (prefijo de servicio: `emr-containers`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EMR on EKS (EMR Containers)
- Tipos de recursos definidos por Amazon EMR on EKS (EMR Containers)
- Claves de condición de Amazon EMR on EKS (EMR Containers)

Acciones definidas por Amazon EMR on EKS (EMR Containers)

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelJobRun	Concede permiso para cancelar una ejecución de trabajo	Escritura	jobRun*		
CreateCertificate	Otorga permiso para crear un certificado	Escritura			
CreateJobTemplate	Concede permiso para crear una plantilla de trabajo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedEndpoint	Otorga permiso para crear un punto de enlace administrado	Escritura	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn	
CreateSecurityConfiguration	Concede permiso para crear una configuración de seguridad	Escritura		aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateVirtualCluster	Otorga permiso para crear un clúster virtual	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJobTemplate	Concede permiso para eliminar una plantilla de trabajo	Escritura	jobTemplate*		
DeleteManagedEndpoint	Otorga permiso para eliminar un punto de enlace administrado	Write	managedEndpoint*		
DeleteVirtualCluster	Otorga permiso para eliminar un clúster virtual	Write	virtualCluster*		
DescribeJobRun	Otorga permiso para describir una ejecución de trabajo	Lectura	jobRun*		
DescribeJobTemplate	Concede permiso para describir una plantilla de trabajo	Lectura	jobTemplate*		
DescribeManagedEndpoint	Otorga permiso para describir un punto de enlace administrado	Lectura	managedEndpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSecurityConfiguration	Concede permiso para describir una configuración de seguridad	Lectura	securityConfiguration*		
DescribeVirtualCluster	Otorga permiso para describir un clúster virtual	Lectura	virtualCluster*		
GetManagedEndpointSessionCredentials	Concede permiso para generar un token de sesión utilizado para conectarse a un punto de conexión administrado	Escritura	managedEndpoint*		
ListJobRuns	Otorga permiso para enumerar las ejecuciones de trabajo asociadas a un clúster virtual	Enumeración	virtualCluster*		
ListJobTemplates	Concede permiso para enumerar las plantillas de trabajo	Enumeración			
ListManagedEndpoints	Otorga permiso para enumerar los puntos de enlace administrados asociados a un clúster virtual	Enumeración	virtualCluster*		
ListSecurityConfigurations	Otorga permiso para enumerar las configuraciones de seguridad	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso especificado	List	jobRun		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			jobTemplate		
			managedEndpoint		
			virtualCluster		
ListVirtualClusters	Otorga permiso para enumerar los clústeres virtuales	List			
StartJobRun	Otorga permiso para iniciar una ejecución de trabajo	Write	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn emr-containers:JobTemplateArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar el recurso especificado	Etiquetado	jobRun		
			jobTemplate		
			managedEndpoint		
			virtualCluster		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para quitar las etiquetas del recurso especificado	Etiquetado	jobRun		
			jobTemplate		
			managedEndpoint		
			virtualCluster		
				aws:TagKeys	

Tipos de recursos definidos por Amazon EMR on EKS (EMR Containers)

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
virtualCluster	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}
jobTemplate	`arn:${Partition}:emr-containers:${Region}:${Account}:/jobtemplates/${JobTemplateId}`	aws:ResourceTag/${TagKey}
managedEndpoint	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/endpoints/${EndpointId}`	aws:ResourceTag/${TagKey}
securityConfiguration	`arn:${Partition}:emr-containers:${Region}:${Account}:/securityconfigurations/${SecurityConfigurationId}`	aws:ResourceTag/${TagKey}
certificate	`arn:${Partition}:emr-containers:${Region}:${Account}:/certificates/${CertificateId}`	

Claves de condición de Amazon EMR on EKS (EMR Containers)

Amazon EMR on EKS (EMR Containers) define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta presentes en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de la etiqueta presentes en la solicitud	ArrayOfString
emr-containers:ExecutionRoleArn	Filtra el acceso por el ARN del rol de ejecución presente en la solicitud	ARN
emr-containers:JobTemplateArn	Filtra el acceso por el ARN de la plantilla de trabajo presente en la solicitud	ARN

Acciones, recursos y claves de condición para Amazon EMR Serverless

Amazon EMR Serverless (prefijo de servicio: `emr-serverless`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EMR Serverless
- Tipos de recursos definidos por Amazon EMR Serverless
- Claves de condición para Amazon EMR Serverless

Acciones definidas por Amazon EMR Serverless

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AccessInteractiveEndpoints [solo permiso]	Concede permiso para ejecutar cargas de trabajo interactivas en una aplicación	Escritura	application*		iam:PassRole
AccessLivyEndpoints [solo permiso]	Concede permiso para ejecutar cargas de trabajo interactivas en un punto de conexión de Livy habilitado en una aplicación sin servidor de EMR	Escritura	application*		iam:PassRole
CancelJobRun	Concede permiso para cancelar una ejecución de trabajo	Escritura	jobRun*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Concede permiso para crear una aplicación	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permiso para eliminar una aplicación.	Escritura	application*		
GetApplication	Concede permiso para obtener una aplicación	Lectura	application*		
GetDashboardForJobRun	Otorga permiso para obtener un panel de ejecución de trabajo	Lectura	jobRun*		
GetJobRun	Concede permiso para obtener una ejecución de trabajo	Lectura	jobRun*		
ListApplications	Concede permiso para enumerar las aplicaciones.	Enumeración			
ListJobRunAttempts	Concede permiso para enumerar los intentos de ejecución de trabajos asociados a una ejecución de trabajo	Enumeración	jobRun*		
ListJobRuns	Concede permiso para mostrar una lista de las ejecuciones de trabajos asociadas a una aplicación	Enumeración	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas del recurso especificado	Lectura	application		
			jobRun		
StartApplication	Concede permiso para iniciar una aplicación	Escritura	application*		
StartJobRun	Concede permiso para iniciar una ejecución de trabajo	Escritura	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	Concede permiso para detener una aplicación	Escritura	application*		
TagResource	Concede permiso para etiquetar el recurso especificado	Etiquetado	application		
			jobRun		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para quitar las etiquetas del recurso especificado	Etiquetado	application		
			jobRun		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	application*		

Tipos de recursos definidos por Amazon EMR Serverless

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon EMR Serverless

Amazon EMR Serverless define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Claves de acciones, recursos y condiciones para la mensajería de usuario AWS final (SMS y voz) (versión 2)

AWS La versión 2 de SMS y voz para el usuario final (prefijo de servicio:`sms-voice`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la mensajería por SMS y voz para AWS el usuario final (V2)
- Tipos de recursos definidos por AWS End User Messaging SMS and Voice V2
- Claves de condición para la mensajería por SMS y voz para el usuario AWS final V2

Acciones definidas por la mensajería por SMS y voz para AWS el usuario final (V2)

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateOriginationIdentity	Otorga permiso para asociar un número de teléfono de origen o un ID de remitente a un grupo	Escritura	Pool*		
			PhoneNumber		
			SenderId		
AssociateProtectConfiguration	Concede permiso para asociar una configuración de protección a un conjunto de configuraciones	Escritura	ConfigurationSet*		
			ProtectConfiguration*		
CreateConfigurationSet	Concede permiso para crear un conjunto de configuración	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEventDestination	Otorga permiso para crear un destino de evento dentro de una configuración establecida	Escritura	ConfigurationSet*		iam:PassRole
CreateOptOutList	Otorga permiso para crear una lista de exclusión voluntaria	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreatePool	Otorga permiso para crear un grupo	Escritura	PhoneNumber		sms-voice:TagResource
			SenderId		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectConfiguration	Concede permiso para crear una configuración de protección	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRegistration	Concede permiso para crear un registro	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationAssociation	Concede permiso para asociar un registro a un número de teléfono u otro registro	Escritura	Registration* PhoneNumber		
CreateRegistrationAttachment	Concede permiso para crear un adjunto de registro	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationVersion	Concede permiso para crear una versión de registro	Escritura	Registration*		
CreateVerifiedDestinationNumber	Concede permiso para crear un número de destino verificado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccountDefaultProtectConfiguration	Concede permiso para eliminar la configuración de protección predeterminada de la cuenta	Escritura			
DeleteConfigurationSet	Otorga permiso para eliminar una configuración establecida	Escritura	ConfigurationSet*		
DeleteDefaultMessageType	Otorga permiso para eliminar el tipo de mensaje predeterminado de una configuración establecida	Escritura	ConfigurationSet*		
DeleteDefaultSenderId	Otorga permiso para eliminar el ID de remitente predeterminado de una configuración establecida	Escritura	ConfigurationSet*		
DeleteEventDestination	Otorga permiso para eliminar un destino para eventos de una configuración establecida	Escritura	ConfigurationSet*		
DeleteKeyword	Otorga permiso para eliminar una palabra clave para un grupo o un número de teléfono de origen	Escritura	PhoneNumber		
			Pool		
DeleteMediaMessageSpendLimitOverride	Concede permiso para eliminar una anulación del límite mensual de gasto en mensajería multimedia de la cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteOptOutList	Otorga permiso para eliminar una lista de exclusión voluntaria	Escritura	OptOutList*		
DeleteOptedOutNumber	Otorga permiso para eliminar un número de teléfono de destino de una lista de exclusión	Escritura	OptOutList*		
DeletePool	Otorga permiso para eliminar un grupo	Escritura	Pool*		
DeleteProtectConfiguration	Concede permiso para eliminar una configuración de protección	Escritura	ProtectConfiguration*		
DeleteProtectConfigurationRuleSetNumberOverride	Otorga permiso para eliminar la anulación de un número de teléfono para una configuración de protección	Escritura	ProtectConfiguration*		
DeleteRegistration	Concede permiso para eliminar un registro	Escritura	Registration*		
DeleteRegistrationAttachment	Concede permiso para eliminar un adjunto de registro	Escritura	RegistrationAttachment*		
DeleteRegistrationFieldValue	Concede permiso para eliminar un valor de campo de registro opcional	Escritura	Registration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos	Administración de permisos	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
DeleteTextMessageSpendLimitOverride	Otorga permiso para eliminar una anulación del límite de gasto mensual de mensajería de texto de su cuenta	Escritura			
DeleteVerifiedDestinationNumber	Concede permiso para eliminar un número de destino verificado	Escritura	VerifiedDestinationNumber*		
DeleteVoiceMessageSpendLimitOverride	Otorga permiso para eliminar una anulación del límite de gasto mensual de mensajería de voz de su cuenta	Escritura			
DescribeAccountAttributes	Otorga permiso para describir los atributos de la cuenta	Lectura			
DescribeAccountLimits	Otorga permiso para describir las Service Quotas para su cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConfigurationSets	Otorga permiso para describir todos los conjuntos de configuración de su cuenta	Lectura	ConfigurationSet		
DescribeKeywords	Otorga permiso para describir las palabras clave de un grupo o un número de teléfono de origen	Lectura	PhoneNumber		
			Pool		
DescribeOptOutLists	Otorga permiso para describir las listas de exclusión de su cuenta	Lectura	OptOutList		
DescribeOptedOutNumbers	Otorga permiso para describir los números de teléfono de destino en una lista de exclusión voluntaria	Lectura	OptOutList*		
DescribePhoneNumbers	Otorga permiso para describir los números de teléfono de origen en su cuenta	Lectura	PhoneNumber		
DescribePools	Otorga permiso para describir los grupos de su cuenta	Lectura	Pool		
DescribeProtectConfigurations	Concede permiso para describir las configuraciones de protección en la cuenta	Lectura	ProtectConfiguration		
DescribeRegistrationAttachments	Concede permiso para describir los adjuntos de registro de su cuenta	Lectura	RegistrationAttachment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRegistrationFieldDefinitions	Concede permiso para describir las definiciones de campos para un tipo de registro determinado	Lectura			
DescribeRegistrationFieldValues	Concede permiso para describir los valores de campos de un registro determinado	Lectura	Registration*		
DescribeRegistrationSectionDefinitions	Concede permiso para describir las definiciones de secciones para un tipo de registro determinado	Lectura			
DescribeRegistrationTypeDefinitions	Concede permiso para describir los tipos de registro compatibles con el servicio	Lectura			
DescribeRegistrationVersions	Concede permiso para describir las versiones de un registro determinado	Lectura	Registration*		
DescribeRegistrations	Concede permiso para describir los registros de su cuenta	Lectura	Registration		
DescribeSenderIds	Otorga permiso para describir al remitente IDs en tu cuenta	Lectura	SenderId		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSpendLimits	Otorga permiso para describir los límites de gasto mensual de su cuenta	Lectura			
DescribeVerifiedDestinationNumbers	Concede permiso para describir los números de destino verificados de su cuenta	Lectura	VerifiedDestinationNumber		
DisassociateOriginationIdentity	Otorga permiso para desasociar un número de teléfono de origen o un ID de remitente de un grupo	Escritura	Pool*		
			PhoneNumber		
			SenderId		
DisassociateProtectConfiguration	Concede permiso para desasociar una configuración de protección de un conjunto de configuraciones	Escritura	ConfigurationSet*		
			ProtectConfiguration*		
DiscardRegistrationVersion	Concede permiso para descartar la última versión de un registro determinado	Escritura	Registration*		
GetProtectConfigurationCountryRuleSet	Concede permiso para obtener el conjunto de reglas del país para una configuración de protección	Lectura	ProtectConfiguration*		
GetResourcePolicy	Otorga permiso para obtener una política de recursos.	Lectura	OptOutList		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			PhoneNumber		
			Pool		
			SenderId		
ListPoolOriginationIdentities	Otorga permiso para incluir todos los números de teléfono de origen y el remitente IDs asociados a un grupo	Lectura	Pool*		
ListProtectConfigurationRuleSetNumberOverrides	Otorga permiso para enumerar todas las anulaciones de números de teléfono para una configuración de protección	Lectura	ProtectConfiguration*		
ListRegistrationAssociations	Concede permiso para enumerar todos los recursos asociados a un registro	Lectura	Registration*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
PutKeyword	Otorga permiso para crear o actualizar una palabra clave para un grupo o un número de teléfono de origen	Escritura	PhoneNumber		
			Pool		
PutMessageFeedback	Otorga permiso para incluir comentarios en un mensaje de texto, voz o multimedia	Escritura	Message*		
PutOptedOutNumber	Otorga permiso para incluir un número de teléfono de destino en una lista de exclusión voluntaria	Escritura	OptOutList*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutProtectConfigurationRuleSetNumberOverride	Otorga permiso para anular un número de teléfono para una configuración de protección	Escritura	ProtectConfiguration*		
PutRegistrationFieldValue	Concede permiso para poner un valor de campo de registro	Escritura	Registration*		
PutResourcePolicy	Concede permiso para colocar una política de recursos	Administración de permisos	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
ReleasePhoneNumber	Otorga permiso para publicar un número de teléfono de origen	Escritura	PhoneNumber*		
ReleaseSenderId	Concede permiso para liberar un ID de remitente	Escritura	SenderId*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RequestPhoneNumber	Otorga permiso para solicitar un número de teléfono de origen	Escritura	Pool		sms-voice:AssociateOriginationIdentity sms-voice:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
RequestSenderId	Concede permiso para solicitar un identificador de remitente no registrado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendDestinationNumberVerificationCode	Concede permiso para enviar un mensaje de texto o voz que contenga un código de verificación a un número de teléfono de destino	Escritura	PhoneNumber		sms-voice:SendTextMessage sms-voice:SendVoiceMessage
			Pool		
			SenderId		
SendMediaMessage	Concede permiso para enviar un mensaje multimedia a un número de teléfono de destino	Escritura	PhoneNumber		
			Pool		
SendTextMessage	Otorga permiso para enviar un mensaje de texto a un número de teléfono de destino	Escritura	PhoneNumber		
			Pool		
			SenderId		
SendVoiceMessage	Otorga permiso para enviar un mensaje de voz a un número de teléfono de destino	Escritura	PhoneNumber		
			Pool		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetAccountDefaultProtectConfiguration	Concede permiso para establecer una configuración de protección predeterminada para la cuenta	Escritura	ProtectConfiguration*		
SetDefaultMessageFeedbackEnabled	Otorga permiso para establecer la retroalimentación de mensajes predeterminada para un conjunto de configuraciones	Escritura	ConfigurationSet*		
SetDefaultMessageType	Otorga permiso para establecer el tipo de mensaje predeterminado para una configuración establecida	Escritura	ConfigurationSet*		
SetDefaultSenderId	Otorga permiso para establecer el ID de remitente predeterminado para una configuración establecida	Escritura	ConfigurationSet*		
SetMediaMessageSpendLimitOverride	Concede permiso para establecer una anulación del límite mensual de gasto en mensajería multimedia de la cuenta	Escritura			
SetTextMessageSpendLimitOverride	Otorga permiso para establecer una anulación para el límite de gasto mensual de mensajería de texto de su cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetVoiceMessageSpendLimitOverride	Otorga permiso para establecer una anulación para el límite de gasto mensual de mensajería de voz de su cuenta	Escritura			
SubmitRegistrationVersion	Concede permiso para enviar la última versión de un registro determinado	Escritura	Registration*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			VerifiedDestinationNumber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			VerifiedDestinationNumber		
				aws:TagKeys	
UpdateEventDestination	Otorga permiso para actualizar el destino del evento de una configuración establecida	Escritura	ConfigurationSet*		iam:PassRole
UpdatePhoneNumber	Otorga permiso para actualizar la configuración de un número de teléfono de origen	Escritura	PhoneNumber*		iam:PassRole
UpdatePool	Otorga permiso para actualizar la configuración de un grupo	Escritura	Pool*		iam:PassRole
UpdateProtectConfiguration	Concede permiso para actualizar una configuración de protección	Escritura	ProtectConfiguration*		
UpdateProtectConfigurationCountryRuleSet	Concede permiso para actualizar un conjunto de reglas del país para una configuración de protección	Escritura	ProtectConfiguration*		
UpdateSenderId	Concede permiso para actualizar la configuración de un identificador del remitente	Escritura	SenderId*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
VerifyDestinationNumber	Concede permiso para verificar un número de teléfono de destino	Escritura	VerifiedDestinationNumber*		

Tipos de recursos definidos por AWS End User Messaging SMS and Voice V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ConfigurationSet	`arn:${Partition}:sms-voice:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
OptOutList	`arn:${Partition}:sms-voice:${Region}:${Account}:opt-out-list/${OptOutListName}`	aws:ResourceTag/${TagKey}
PhoneNumber	`arn:${Partition}:sms-voice:${Region}:${Account}:phone-number/${PhoneNumberId}`	aws:ResourceTag/${TagKey}
Pool	`arn:${Partition}:sms-voice:${Region}:${Account}:pool/${PoolId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
ProtectConfiguration	`arn:${Partition}:sms-voice:${Region}:${Account}:protect-configuration/${ProtectConfigurationId}`	aws:ResourceTag/${TagKey}
SenderId	`arn:${Partition}:sms-voice:${Region}:${Account}:sender-id/${SenderId}/${IsoCountryCode}`	aws:ResourceTag/${TagKey}
Registration	`arn:${Partition}:sms-voice:${Region}:${Account}:registration/${RegistrationId}`	aws:ResourceTag/${TagKey}
RegistrationAttachment	`arn:${Partition}:sms-voice:${Region}:${Account}:registration-attachment/${RegistrationAttachmentId}`	aws:ResourceTag/${TagKey}
VerifiedDestinationNumber	`arn:${Partition}:sms-voice:${Region}:${Account}:verified-destination-number/${VerifiedDestinationNumberId}`	aws:ResourceTag/${TagKey}
Message	`arn:${Partition}:sms-voice:${Region}:${Account}:message/${MessageId}`	

Claves de condición para la mensajería por SMS y voz para el usuario AWS final V2

AWS La versión V2 de mensajería de usuario final por SMS y voz define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Mensajes de redes sociales para usuarios finales de AWS

AWS End User Messaging Social (prefijo de servicio:`social-messaging`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Mensajes de redes sociales para usuarios finales de AWS
- Tipos de recursos definidos por Mensajes de redes sociales para usuarios finales de AWS
- Claves de condición de Mensajes de redes sociales para usuarios finales de AWS

Acciones definidas por Mensajes de redes sociales para usuarios finales de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateWhatsAppBusinessAccount	Otorga permiso para asociar una cuenta WhatsApp empresarial a su Cuenta de AWS	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteWhatsAppMessageMedia	Otorga permiso para eliminar un objeto multimedia de WhatsApp	Escritura	phone-number-id*		
DisassociateWhatsAppBusinessAccount	Otorga permiso para desvincular una cuenta WhatsApp empresarial de la suya Cuenta de AWS	Escritura	waba*		
GetLinkedWhatsAppBusinessAccount	Otorga permiso para ver los detalles de una cuenta WhatsApp empresarial	Lectura	waba*		
GetLinkedWhatsAppBusinessAccountPhoneNumber	Concede permiso para ver los detalles de un número de teléfono	Lectura	phone-number-id*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetWhatsAppMessageMedia	Otorga permiso para obtener un objeto multimedia de WhatsApp	Escritura	phone-number-id*		
ListLinkedWhatsAppBusinessAccounts	Otorga permiso para ver todas tus cuentas WhatsApp empresariales	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	phone-number-id		
			waba		
PostWhatsAppMessageMedia	Otorga permiso para cargar un objeto multimedia en WhatsApp	Escritura	phone-number-id*		
PutWhatsAppBusinessAccountEventDestinations	Otorga permiso para actualizar el destino WhatsApp de un evento de Business Accounts	Escritura	waba*		
SendWhatsAppMessage	Otorga permiso para enviar un mensaje a través WhatsApp	Escritura	phone-number-id*		
TagResource	Otorga permiso para agregar una etiqueta a un recurso.	Etiquetado	phone-number-id		
			waba		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	phone-number-id		
			waba		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por Mensajes de redes sociales para usuarios finales de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
phone-number-id	`arn:${Partition}:social-messaging:${Region}:${Account}:phone-number-id/${OriginationPhoneNumberId}`	aws:ResourceTag/${TagKey}
waba	`arn:${Partition}:social-messaging:${Region}:${Account}:waba/${WabaId}`	aws:ResourceTag/${TagKey}

Claves de condición de Mensajes de redes sociales para usuarios finales de AWS

AWS End User Messaging Social define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Entity Resolution

AWS Entity Resolution (prefijo de servicio:`entityresolution`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Entity Resolution
- Tipos de recursos definidos por AWS Entity Resolution
- Claves de condición para AWS Entity Resolution

Acciones definidas por AWS Entity Resolution

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddPolicyStatement	Otorga permiso para dar permiso a un AWS servicio u otra cuenta para usar los recursos de una AWS Entity Resolution	Administración de permisos			
BatchDeleteUniqueId	Concede permiso para eliminar por lotes un ID único	Escritura	MatchingWorkflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIdMappingWorkflow	Concede permiso para crear un flujo de trabajo de idmapping	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIdNamespace	Otorga permiso para crear un IdNamespace	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMatchingWorkflow	Otorga permiso para crear un flujo de trabajo coincidente	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchemaMapping	Otorga permiso para crear una asignación de esquema	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdMappingWorkflow	Concede permiso para eliminar un flujo de trabajo de idmapping	Escritura	IdMappingWorkflow*		
DeleteIdNamespace	Otorga permiso para eliminar un IdNamespace	Escritura	IdNamespace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMatchingWorkflow	Otorga permiso para eliminar un flujo de trabajo coincidente	Escritura	MatchingWorkflow*		
DeletePolicyStatement	Otorga permiso para eliminar el permiso otorgado a un AWS servicio o permiso a otra cuenta para usar los recursos de una AWS Entity Resolution	Administración de permisos			
DeleteSchemaMapping	Otorga permiso para eliminar una asignación de esquema	Escritura	SchemaMapping*		
GenerateMatchId	Otorga permiso para generar un identificador de coincidencia	Escritura	MatchingWorkflow*		
GetIdMappingJob	Concede permiso para obtener trabajo de idmapping	Lectura	IdMappingWorkflow*		
GetIdMappingWorkflow	Concede permiso para obtener un flujo de trabajo de idmapping	Lectura	IdMappingWorkflow*		
GetIdNamespace	Otorga permiso para obtener un IdNamespace	Lectura	IdNamespace*		
GetMatchId	Otorga permiso para obtener un ID de coincidencia	Lectura	MatchingWorkflow*		
GetMatchingJob	Otorga permiso para obtener un trabajo coincidente	Lectura	MatchingWorkflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMatchingWorkflow	Otorga permiso para obtener un flujo de trabajo coincidente	Lectura	MatchingWorkflow*		
GetPolicy	Otorga permiso para obtener una política de recursos para los recursos de una AWS entidad Resolution	Lectura			
GetProviderService	Concede permiso para obtener el servicio de proveedor	Lectura	ProviderService*		
GetSchemaMapping	Otorga permiso para obtener una asignación de esquema	Lectura	SchemaMapping*		
ListIdMappingJobs	Concede permiso para enumerar trabajos de idmapping	Enumeración	IdMappingWorkflow*		
ListIdMappingWorkflows	Concede permiso para enumerar flujos de trabajo de idmapping	Enumeración			
ListIdNamespaces	Otorga permiso para publicar IdNamespaces	Enumeración			
ListMatchingJobs	Otorga permiso para listar trabajos coincidentes	Enumeración	MatchingWorkflow*		
ListMatchingWorkflows	Otorga permiso para enumerar flujos de trabajo coincidentes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProviderServices	Concede permiso para enumerar los servicios de proveedor	Enumeración			
ListSchemaMappings	Otorga permiso para enumerar las asignaciones de esquemas	Enumeración			
ListTagsForResource	Otorga permiso para enumerar etiquetas para un recurso	Lectura			
PutPolicy	Otorga permiso para establecer una política de recursos para un recurso de AWS Entity Resolution	Administración de permisos			
StartIdMappingJob	Concede permiso para comenzar un trabajo de idmapping	Escritura	IdMappingWorkflow*		
StartMatchingJob	Otorga permiso para iniciar un trabajo coincidente	Escritura	MatchingWorkflow*		
TagResource	Concede permiso para agregar etiquetas a un recurso	Etiquetado	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ProviderService		
			SchemaMapping		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:TagKeys	
UpdateIdMappingWorkflow	Concede permiso para actualizar un flujo de trabajo de idmapping	Escritura	IdMappingWorkflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIdNamespace	Otorga permiso para actualizar un IdNamespace	Escritura	IdNamespace*		
UpdateMatchingWorkflow	Otorga permiso para actualizar un flujo de trabajo coincidente	Escritura	MatchingWorkflow*		
UpdateSchemaMapping	Concede permiso para actualizar una asignación de esquema	Escritura	SchemaMapping*		
UseIdNamespace	Otorga permiso para usar un AWS servicio u otra cuenta IdNamespace en un flujo de trabajo	Administración de permisos			
UseWorkflow	Otorga permiso para conceder permiso a un AWS servicio u otra cuenta para usar el flujo de trabajo dentro de un IdNamespace	Administración de permisos			

Tipos de recursos definidos por AWS Entity Resolution

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
MatchingWorkflow	`arn:${Partition}:entityresolution:${Region}:${Account}:matchingworkflow/${WorkflowName}`	aws:ResourceTag/${TagKey}
SchemaMapping	`arn:${Partition}:entityresolution:${Region}:${Account}:schemamapping/${SchemaName}`	aws:ResourceTag/${TagKey}
IdMappingWorkflow	`arn:${Partition}:entityresolution:${Region}:${Account}:idmappingworkflow/${WorkflowName}`	aws:ResourceTag/${TagKey}
ProviderService	`arn:${Partition}:entityresolution:${Region}:${Account}:providerservice/${ProviderName}/${ProviderServiceName}`	aws:ResourceTag/${TagKey}
IdNamespace	`arn:${Partition}:entityresolution:${Region}:${Account}:idnamespace/${IdNamespaceName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Entity Resolution

AWS Entity Resolution define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por una clave que está presente en la solicitud que el usuario realiza al servicio de resolución de entidades	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena
aws:TagKeys	Filtra el acceso mediante la lista de todos los nombres de clave de etiqueta presentes en la solicitud que el usuario realiza al servicio de resolución de identidades	ArrayOfString

Acciones, recursos y claves de condición de Amazon EventBridge

Amazon EventBridge (prefijo de servicio:`events`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EventBridge
- Tipos de recursos definidos por Amazon EventBridge
- Claves de estado de Amazon EventBridge

Acciones definidas por Amazon EventBridge

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateEventSource	Concede permiso para activar orígenes de eventos de socios	Write	event-source*		
CancelReplay	Concede permiso para cancelar una repetición	Write	replay*		
CreateApiDestination	Concede permiso para crear un nuevo destino de API.	Write	api-destination*		
			connection*		
CreateArchive	Concede permiso para crear un nuevo archivo	Write	archive*		
			event-bus*		
			alias		
			key		
CreateConnection	Concede permiso para crear una conexión nueva.	Escritura	connection*		
CreateEndpoint	Concede permiso para crear un nuevo punto de conexión	Escritura	endpoint*		
				events:EventBusArn	
CreateEventBus	Concede permiso para crear buses de eventos	Write	event-bus*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerEventSource	Concede permiso para crear orígenes de eventos de socios	Write	event-source*		
DeactivateEventSource	Concede permiso para desactivar orígenes de eventos	Write	event-source*		
DeauthorizeConnection	Concede permiso para cancelar la autorización de una conexión y eliminar sus secretos de autorización almacenados	Write	connection*		
DeleteApiDestination	Concede permiso para eliminar un destino de API.	Write	api-destination*		
DeleteArchive	Concede permiso para eliminar un archivo	Write	archive*		
DeleteConnection	Concede permiso para eliminar una conexión.	Escritura	connection*		
DeleteEndpoint	Concede permiso para eliminar un punto de conexión.	Escritura	endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEventBus	Concede permiso para eliminar buses de eventos	Write	event-bus*		
DeletePartnerEventSource	Concede permiso para eliminar orígenes de eventos de socios	Write	event-source*		
DeleteRule	Concede permiso para eliminar reglas	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
DescribeApiDestination	Concede permiso para recuperar los detalles de un destino de API.	Read	api-destination*		
			connection*		
DescribeArchive	Concede permiso para recuperar los detalles de un archivo	Read	archive*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConnection	Concede permiso para recuperar los detalles de una conexión.	Lectura	connection*		
DescribeEndpoint	Concede permiso para recuperar los detalles de un punto de conexión	Lectura	endpoint*		
DescribeEventBus	Concede permiso para recuperar los detalles de los buses de eventos	Read	event-bus		
DescribeEventSource	Concede permiso para recuperar los detalles de los orígenes de eventos	Read	event-source*		
DescribePartnerEventSource	Concede permiso para recuperar los detalles de los orígenes de eventos de socios	Read	event-source*		
DescribeReplay	Concede permiso para recuperar los detalles de una repetición	Read	replay*		
DescribeRule	Concede permiso para recuperar los detalles de las reglas	Read	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				events:creatorAccount	
DisableRule	Concede permiso para desactivar reglas	Escritura	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
EnableRule	Concede permiso para habilitar reglas.	Escritura	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				events:creatorAccount events:ManagedBy	
InvokeApiDestination [solo permiso]	Concede permiso para invocar un destino de API.	Write	api-destination*		
ListApiDestinations	Concede permiso para recuperar una lista de destinos de API.	List			
ListArchives	Concede permiso para recuperar una lista de archivos	List			
ListConnections	Concede permiso para recuperar una lista de conexiones.	Enumeración			
ListEndpoints	Concede permiso para recuperar una lista de puntos de conexión	Enumeración			
ListEventBuses	Concede permiso para recuperar una lista de los buses de eventos de su cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEventSources	Concede permiso para recuperar una lista de los orígenes de eventos compartidos con esta cuenta	Enumeración			
ListPartnerEventSourceAccounts	Otorga permiso para recuperar una lista de Cuenta de AWS IDs fuentes asociadas a un evento	Enumeración	event-source*		
ListPartnerEventSources	Concede permiso para recuperar una lista de los orígenes de eventos de socios	List			
ListReplays	Concede permiso para recuperar una lista de las repeticiones	List			
ListRuleNamesByTarget	Concede permiso para recuperar una lista de los nombres de las reglas asociadas a un destino	Enumeración			
ListRules	Otorga permiso para recuperar una lista de las EventBridge reglas de Amazon de la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para recuperar una lista de etiquetas asociadas a un EventBridge recurso de Amazon	Enumeración	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
ListTargetsByRule	Concede permiso para recuperar una lista de los destinos definidos para una regla	Enumeración	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
PutEvents	Otorga permiso para enviar eventos personalizados a Amazon EventBridge	Escritura	event-bus*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				events:detail-type events:source events:eventBusInvocation	
PutPartnerEvents	Otorga permiso para enviar eventos personalizados a Amazon EventBridge	Escritura			
PutPermission	Otorga permiso para usar la PutPermission acción y permite Cuenta de AWS a otra persona colocar los eventos en tu bus de eventos predeterminado	Administración de permisos			
PutRule	Concede permiso para crear o actualizar reglas	Escritura	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutTargets	Concede permiso para agregar destinos a una regla	Escritura	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	Otorga permiso para revocar el permiso de otra persona Cuenta de AWS para colocar eventos en tu bus de eventos predeterminado	Administración de permisos			
RemoveTargets	Concede permiso para eliminar destinos de una regla	Escritura	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [solo permiso]	Concede permiso para recuperar las credenciales de una conexión	Escritura	connection*		
StartReplay	Concede permiso para iniciar la repetición de un archivo	Escritura	archive*		
			event-bus*		
			replay*		
TagResource	Otorga permiso para añadir una etiqueta a un EventBridge recurso de Amazon	Etiquetado	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	Concede permiso para probar si un patrón de eventos coincide con el evento proporcionado.	Lectura			
UntagResource	Otorga permiso para eliminar una etiqueta de un EventBridge recurso de Amazon	Etiquetado	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApiDestination	Concede permiso para actualizar un destino de API.	Write	api-destination*		
UpdateArchive	Concede permiso para actualizar un archivo	Write	archive*		
			alias		
			key		
UpdateConnection	Concede permiso para actualizar una conexión.	Escritura	connection*		
UpdateEndpoint	Concede permiso para actualizar un punto de conexión	Escritura	endpoint*		
				events:EventBusArn	
UpdateEventBus	Concede permiso para actualizar buses de eventos	Escritura	event-bus*		

Tipos de recursos definidos por Amazon EventBridge

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
event-source	arn:${Partition}:events:${Region}::event-source/${EventSourceName}	
event-bus	arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}	aws:ResourceTag/${TagKey}
rule-on-default-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${RuleName}	aws:ResourceTag/${TagKey}
rule-on-custom-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}	aws:ResourceTag/${TagKey}
archive	arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}	
replay	arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}	
connection	arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}	
api-destination	arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}	
endpoint	arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}	
create-snapshot	arn:${Partition}:events:${Region}:${Account}:target/create-snapshot	
reboot-instance	arn:${Partition}:events:${Region}:${Account}:target/reboot-instance	

Tipos de recurso	ARN	Claves de condición
stop-instance	`arn:${Partition}:events:${Region}:${Account}:target/stop-instance`	
terminate-instance	`arn:${Partition}:events:${Region}:${Account}:target/terminate-instance`	
alias	`arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}`	
key	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

Claves de estado de Amazon EventBridge

Amazon EventBridge define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según del conjunto de valores permitido para cada una de las etiquetas al bus de eventos y acciones de reglas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor de la etiqueta asociada con el recurso al bus de eventos y acciones de reglas.	Cadena
aws:TagKeys	Filtra el acceso según la presencia de etiquetas obligatorias en la solicitud al bus de eventos y acciones de reglas.	ArrayOfString

Claves de condición	Descripción	Tipo
events:EventBusArn	Filtra el acceso por el ARN de los buses de eventos que se pueden asociar a CreateEndpoint un punto final y las acciones UpdateEndpoint	ArrayOfARN
events:ManagedBy	Filtra el acceso por AWS servicios. Si un AWS servicio crea una regla en su nombre, el valor es el nombre principal del servicio que creó la regla	Cadena
events:TargetArn	Filtra el acceso por el ARN de un objetivo que se puede establecer en una regla de acciones. PutTargets TargetARN no incluye DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	Filtra el acceso según la cuenta en la que se creó la regla a las acciones de reglas.	Cadena
events:detail-type	Filtra el acceso por la cadena literal del tipo de detalle del evento y las acciones PutEvents PutRule	Cadena
events:detail.eventTypeCode	Filtra el acceso por la cadena literal del detalle. eventTypeCode campo del evento para PutRule acciones	Cadena
events:detail.service	Filtra el acceso a las acciones mediante la cadena literal del campo detail.service del evento PutRule	Cadena
events:detail.userIdentity.principalId	Filtra el acceso a las acciones mediante la cadena literal del campo detail.useridentity.principalid del evento PutRule	Cadena
events:eventBusInvocation	Filtra el acceso en función de si el evento se generó mediante una API o mediante la invocación de acciones a través de un bus multicuenta PutEvents	Cadena

Claves de condición	Descripción	Tipo
events:source	Filtra el acceso según el AWS servicio o la fuente del evento AWS asociado que generó el evento PutEvents y PutRule las acciones. Coincide con la cadena literal del campo de origen del evento.	ArrayOfString

Acciones, recursos y claves de condición de Amazon EventBridge Pipes

Amazon EventBridge Pipes (prefijo de servicio:`pipes`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EventBridge Pipes
- Tipos de recursos definidos por Amazon EventBridge Pipes
- Claves de estado de Amazon EventBridge Pipes

Acciones definidas por Amazon EventBridge Pipes

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePipe	Otorga permiso para crear una canalización	Escritura	pipe*		iam:PassRole
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeletePipe	Otorga permiso para eliminar una canalización	Escritura	pipe*		
				aws:ResourceTag/${TagKey}	
DescribePipe	Otorga permiso para describir una canalización	Lectura	pipe*		
				aws:ResourceTag/${TagKey}	
ListPipes	Otorga permiso para enumerar todas las canalizaciones de su cuenta	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	pipe*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
StartPipe	Otorga permiso para iniciar una canalización	Escritura	pipe*		
				aws:ResourceTag/${TagKey}	
StopPipe	Otorga permiso para detener una canalización	Escritura	pipe*		
				aws:ResourceTag/${TagKey}	
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	pipe*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	pipe*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePipe	Otorga permiso para actualizar una canalización	Escritura	pipe*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon EventBridge Pipes

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
pipe	`arn:${Partition}:pipes:${Region}:${Account}:pipe/${Name}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon EventBridge Pipes

Amazon EventBridge Pipes define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon EventBridge Scheduler

Amazon EventBridge Scheduler (prefijo de servicio:`scheduler`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EventBridge Scheduler
- Tipos de recursos definidos por Amazon EventBridge Scheduler
- Claves de condición de Amazon EventBridge Scheduler

Acciones definidas por Amazon EventBridge Scheduler

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSchedule	Otorga permiso para crear un horario de Amazon EventBridge Scheduler	Escritura	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	
CreateScheduleGroup	Otorga permiso para crear un grupo de programación de Amazon EventBridge Scheduler	Escritura	schedule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSchedule	Otorga permiso para eliminar una programación de Amazon EventBridge Scheduler	Escritura	schedule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeleteScheduleGroup	Otorga permiso para eliminar un grupo de programación de Amazon EventBridge Scheduler	Escritura	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Otorga permiso para ver los detalles de una programación de Amazon EventBridge Scheduler	Lectura	schedule*		
				aws:ResourceTag/${TagKey}	
GetScheduleGroup	Otorga permiso para ver detalles sobre un grupo de programación de Amazon EventBridge Scheduler	Lectura	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	Otorga permiso para incluir los grupos de programación de Amazon EventBridge Scheduler en su cuenta	Enumeración			
ListSchedules	Otorga permiso para incluir los horarios de Amazon EventBridge Scheduler en su cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso a la etiqueta de listas para un recurso de Amazon EventBridge Scheduler	Lectura	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Otorga permiso para etiquetar un recurso de Amazon EventBridge Scheduler	Etiquetado	schedule-group*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para desetiquetar un recurso de Amazon EventBridge Scheduler	Etiquetado	schedule-group*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Otorga permiso para modificar una programación de Amazon EventBridge Scheduler	Escritura	schedule*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon EventBridge Scheduler

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
schedule-group	`arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}`	aws:ResourceTag/${TagKey}
schedule	`arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}`	

Claves de condición de Amazon EventBridge Scheduler

Amazon EventBridge Scheduler define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon EventBridge Schemas

Amazon EventBridge Schemas (prefijo de servicio:`schemas`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon EventBridge Schemas
- Tipos de recursos definidos por Amazon EventBridge Schemas
- Claves de condición de Amazon EventBridge Schemas

Acciones definidas por Amazon EventBridge Schemas

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDiscoverer	Otorga permiso para crear un programa de detección de esquemas de eventos. Una vez creado, los eventos se asignarán automáticamente a los documentos de esquema correspondientes.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegistry	Otorga permiso para crear un nuevo registro de esquemas en su cuenta	Escritura	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Otorga permiso para crear un nuevo esquema en su cuenta	Escritura	schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDiscoverer	Otorga permiso para eliminar un programa de detección de su cuenta	Escritura	discoverer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRegistry	Otorga permiso para eliminar un registro existente de la cuenta	Escritura	registry*		
DeleteResourcePolicy	Otorga permiso para eliminar la política basada en recursos asociada a un registro determinado	Escritura	registry*		
DeleteSchema	Otorga permiso para eliminar un esquema existente en su cuenta	Escritura	schema*		
DeleteSchemaVersion	Otorga permiso para eliminar una versión específica del esquema de la cuenta	Escritura	schema*		
DescribeCodeBinding	Otorga permiso para recuperar metadatos del código generado para un esquema específico de la cuenta	Lectura	schema*		
DescribeDiscoverer	Otorga permiso para recuperar metadatos de detección de la cuenta	Lectura	discoverer*		
DescribeRegistry	Otorga permiso para describir los metadatos de un registro existentes en la cuenta	Lectura	registry*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSchema	Otorga permiso para recuperar un esquema existente en la cuenta	Lectura	schema*		
ExportSchema	Otorga permiso para exportar el AWS registro o los esquemas descubiertos en formato OpenAPI 3 a formato JSONSchema	Lectura	registry*		
			schema*		
GetCodeBindingSource	Otorga permiso para recuperar metadatos del código generado para un esquema específico de la cuenta	Lectura	schema*		
GetDiscoveredSchema	Otorga permiso para recuperar el esquema de la lista de eventos de ejemplo proporcionada	Lectura			
GetResourcePolicy	Otorga permiso para recuperar la política basada en recursos asociada a un registro determinado	Lectura	registry*		
ListDiscoverers	Otorga permiso para mostrar una lista de todos los programas de detección en su cuenta	Enumeración	discoverer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRegistries	Otorga permiso para mostrar una lista de todos los registros de su cuenta	Enumeración	registry*		
ListSchemaVersions	Otorga permiso para mostrar una lista de todas las versiones de un esquema	Enumeración	schema*		
ListSchemas	Otorga permiso para mostrar una lista de todos los esquemas	Enumeración	schema*		
ListTagsForResource	Otorga permiso para mostrar una lista de las etiquetas para un recurso	Lectura	discoverer		
			registry		
			schema		
PutCodeBinding	Otorga permiso para generar un código para un esquema específico de la cuenta	Escritura	schema*		
PutResourcePolicy	Otorga permiso para adjuntar una política basada en recursos a un registro determinado	Escritura	registry*		
SearchSchemas	Otorga permiso para buscar esquemas en función de palabras clave específicas de la cuenta	Enumeración	schema*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDiscoverer	Otorga permiso para iniciar la detección especificada. Una vez iniciado, el programa registra automáticamente los esquemas de los eventos publicados en el origen configurado en la cuenta.	Escritura	discoverer*		
StopDiscoverer	Otorga permiso para detener la detección especificada. Una vez iniciada la detección, el programa ya no registra los esquemas de los eventos publicados en el origen configurado en la cuenta	Escritura	discoverer*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	discoverer		
			registry		
			schema		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	discoverer		
			registry		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			schema		
				aws:TagKeys	
UpdateDiscoverer	Otorga permiso para actualizar un programa de detección existente en la cuenta	Escritura	discoverer*		
UpdateRegistry	Otorga permiso para actualizar los metadatos de un registro existentes en la cuenta	Escritura	registry*		
UpdateSchema	Otorga permiso para actualizar un esquema existente en su cuenta	Escritura	schema*		

Tipos de recursos definidos por Amazon EventBridge Schemas

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
discoverer	`arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
registry	`arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}`	aws:ResourceTag/${TagKey}
schema	`arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon EventBridge Schemas

Amazon EventBridge Schemas define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el servicio de inserción de errores de AWS

AWS El servicio de inyección de errores (prefijo de servicio:`fis`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el simulador de inserción de errores de AWS
- Tipos de recursos definidos por el servicio de inserción de errores de AWS
- Claves de condición para el servicio de inserción de errores de AWS

Acciones definidas por el simulador de inserción de errores de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateExperimentTemplate	Otorga permiso para crear una plantilla de experimento AWS del FIS	Escritura	action*		
			experiment-template*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateTargetAccountConfiguration	Otorga permiso para crear una configuración de cuenta de destino AWS de la FIS	Escritura	experiment-template*		
DeleteExperimentTemplate	Concede permiso para eliminar la plantilla del experimento de la AWS FIS	Escritura	experiment-template*		
DeleteTargetAccountConfiguration	Otorga permiso para eliminar la configuración de una cuenta AWS de destino de la FIS	Escritura	experiment-template*		
GetAction	Otorga permiso para recuperar una acción de la AWS FIS	Lectura	action*		
				aws:ResourceTag/${TagKey}	
GetExperiment	Otorga permiso para recuperar un experimento del AWS FIS	Lectura	experiment*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetExperimentTargetAccountConfiguration	Otorga permiso para recuperar la configuración de una cuenta AWS objetivo del FIS para un AWS experimento del FIS	Lectura	experiment*		
GetExperimentTemplate	Otorga permiso para recuperar una plantilla de experimento del AWS FIS	Lectura	experiment-template*		
				aws:ResourceTag/${TagKey}	
GetSafetyLever	Concede permiso para obtener información sobre la palanca de seguridad	Lectura	safety-lever*		
GetTargetAccountConfiguration	Otorga permiso para recuperar la configuración de una cuenta AWS objetivo del FIS para una plantilla de experimento del AWS FIS	Lectura	experiment-template*		
GetTargetResourceType	Concede permiso para obtener información sobre el tipo de recurso especificado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InjectApiInternalError [solo permiso]	Otorga permiso para introducir un error interno de API en el AWS servicio proporcionado a partir de un experimento de FIS	Escritura	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiThrottleError [solo permiso]	Otorga permiso para introducir un error de aceleración de la API en el AWS servicio proporcionado a partir de un experimento de la FIS	Escritura	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InjectApiUnavailableError [solo permiso]	Otorga permiso para introducir un error de API no disponible en el AWS servicio proporcionado a partir de un experimento de la FIS	Escritura	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
ListActions	Otorga permiso para enumerar todas las acciones de la FIS disponibles AWS	Enumeración			
ListExperimentResolvedTargets	Otorga permiso para enumerar los objetivos resueltos para los experimentos del AWS FIS	Enumeración	experiment*		
ListExperimentTargetAccountConfigurations	Otorga permiso para enumerar las configuraciones de cuentas de destino para los experimentos del AWS FIS	Enumeración	experiment*		
ListExperimentTemplates	Otorga permiso para enumerar todas las plantillas de experimentos AWS del FIS disponibles	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExperiments	Otorga permiso para enumerar todos los experimentos del AWS FIS disponibles	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso del AWS FIS	Lectura	action		
			experiment		
			experiment-template		
ListTargetAccountConfigurations	Otorga permiso para enumerar las configuraciones de cuentas de destino para las plantillas de AWS experimentos del FIS	Enumeración	experiment-template*		
ListTargetResourceTypes	Concede permiso para enumerar los tipos de recursos	Enumeración			
StartExperiment	Otorga permiso para ejecutar un experimento del AWS FIS	Escritura	experiment*		iam:CreateServiceLinkedRole
			experiment-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
StopExperiment	Otorga permiso para detener un experimento del AWS FIS	Escritura	experiment*		
TagResource	Otorga permiso para etiquetar los recursos del AWS FIS	Etiquetado	action		
			experiment		
			experiment-template		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para desetiquetar los recursos AWS del FIS	Etiquetado	action		
			experiment		
			experiment-template		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateExperimentTemplate	Otorga permiso para actualizar la plantilla de experimento del AWS FIS especificada	Escritura	experiment-template*		
			action		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSafetyLeverState	Concede permiso para actualizar el estado de la palanca de seguridad	Escritura	safety-lever*		
UpdateTargetAccountConfiguration	Otorga permiso para actualizar la configuración de una cuenta AWS de destino de la FIS	Escritura	experiment-template*		

Tipos de recursos definidos por el servicio de inserción de errores de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
action	arn:${Partition}:fis:${Region}:${Account}:action/${Id}	aws:ResourceTag/${TagKey}
experiment	arn:${Partition}:fis:${Region}:${Account}:experiment/${Id}	aws:ResourceTag/${TagKey}
experiment-template	arn:${Partition}:fis:${Region}:${Account}:experiment-template/${Id}	aws:ResourceTag/${TagKey}
safety-lever	arn:${Partition}:fis:${Region}:${Account}:safety-lever/${Id}	

Claves de condición para el servicio de inserción de errores de AWS

AWS El servicio de inyección de errores define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
fis:Operations	Filtra el acceso según la lista de operaciones del AWS servicio que se ven afectadas por la acción del AWS FIS	ArrayOfString
fis:Percentage	Filtra el acceso según el porcentaje de llamadas que se ven afectadas por la acción del AWS FIS	Numérico
fis:Service	Filtra el acceso por el AWS servicio que se ve afectado por la acción del AWS FIS	Cadena
fis:Targets	Filtra el acceso según la lista de recursos a los ARNs que apunta la acción del AWS FIS	ArrayOfString

Acciones, recursos y claves de condición de Amazon FinSpace

Amazon FinSpace (prefijo de servicio:`finspace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon FinSpace
- Tipos de recursos definidos por Amazon FinSpace
- Claves de estado de Amazon FinSpace

Acciones definidas por Amazon FinSpace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConnectKxCluster [solo permiso]	Concede permiso para conectarse a un clúster de kdb	Escritura	kxCluster*		
CreateEnvironment	Otorga permiso para crear un entorno FinSpace	Escritura	environment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxChangeset	Concede permiso para crear un conjunto de cambios para una base de datos de kdb	Escritura	kxDatabase*		
CreateKxCluster	Concede permiso para crear un clúster en un entorno de kdb administrado	Escritura	kxCluster*		ec2:DescribeSubnets finspace:MountKxDatabase
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	
CreateKxDatabase	Concede permiso para crear una base de datos de kdb en un entorno de kdb administrado	Escritura	kxDatabase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDataview	Concede permiso para crear una vista de datos en un entorno de kdb administrado	Escritura	kxDataview*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxEnvironment	Concede permiso para crear un entorno de kdb administrado	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxScalingGroup	Concede permiso para crear un grupo de escalado en un entorno de kdb administrado	Escritura	kxScalingGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxUser	Concede permiso para crear un usuario en un entorno de kdb administrado	Escritura	kxEnvironment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxVolume	Concede permiso para crear un volumen en un entorno de kdb administrado	Escritura	kxVolume*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUser	Otorga permiso para crear un FinSpace usuario	Escritura	environment*		
			user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEnvironment	Otorga permiso para eliminar un FinSpace entorno	Escritura	environment*		
DeleteKxCluster	Concede permiso para eliminar un clúster de kdb	Escritura	kxCluster*		
DeleteKxClusterNode	Concede permiso para eliminar un nodo de un clúster de KDB	Escritura	kxCluster*		
DeleteKxDatabase	Concede permiso para eliminar una base de datos de kdb	Escritura	kxDatabase*		
DeleteKxDataview	Concede permiso para eliminar una vista de datos en un entorno de kdb administrado	Escritura	kxDataview*		
DeleteKxEnvironment	Concede permiso para eliminar un entorno de kdb administrado	Escritura	kxEnvironment*		
DeleteKxScalingGroup	Concede permiso para eliminar un grupo de escalado en un entorno de kdb administrado	Escritura	kxScalingGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteKxUser	Concede permiso para eliminar un usuario de kdb	Escritura	kxUser*		
DeleteKxVolume	Concede permiso para eliminar un volumen en un entorno de kdb administrado	Escritura	kxVolume*		
GetEnvironment	Otorga permiso para describir un FinSpace entorno	Lectura	environment*		
GetKxChangeset	Concede permiso para describir un conjunto de cambios para una base de datos de kdb	Lectura	kxDatabase*		
GetKxCluster	Concede permiso para describir un clúster en un entorno de kdb administrado	Lectura	kxCluster*		
GetKxConnectionString	Concede permiso para recuperar una cadena de conexión para clústeres de kdb	Lectura	kxCluster*		finspace:ConnectKxCluster
GetKxDatabase	Concede permiso para describir una base de datos de kdb	Lectura	kxDatabase*		
GetKxDataview	Concede permiso para describir una vista de datos en un entorno de kdb administrado	Lectura	kxDataview*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetKxEnvironment	Concede permiso para describir un entorno de kdb administrado	Lectura	kxEnvironment*		
GetKxScalingGroup	Concede permiso para describir un grupo de escalado en un entorno de kdb administrado	Lectura	kxScalingGroup*		
GetKxUser	Concede permiso para describir un usuario de kdb	Lectura	kxUser*		
GetKxVolume	Concede permiso para describir un volumen en un entorno de kdb administrado	Lectura	kxVolume*		
GetLoadSampleDataSetGroupIntoEnvironmentStatus	Concede permiso para solicitar el estado de la carga del paquete de datos de muestra	Lectura	environment*		
GetUser	Otorga permiso para describir a un FinSpace usuario	Lectura	environment*		
			user*		
ListEnvironments	Otorga permiso para enumerar FinSpace los entornos en Cuenta de AWS	Enumeración	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListKxChangesets	Concede permiso para enumerar los conjuntos de cambios para una base de datos de kdb	Enumeración	kxDatabase*		
ListKxClusterNodes	Concede permiso para enumerar los nodos del clúster en un entorno de kdb administrado	Enumeración	kxCluster*		
ListKxClusters	Concede permiso para enumerar los clústeres en un entorno de kdb administrado	Enumeración	kxEnvironment*		
ListKxDatabases	Concede permiso para enumerar las bases de datos de kdb en un entorno de kdb administrado	Enumeración	kxEnvironment*		
ListKxDataviews	Concede permiso para mostrar vistas de datos en una base de datos	Enumeración	kxDatabase*		
ListKxEnvironments	Concede permiso para enumerar los entornos de kdb administrados	Enumeración			
ListKxScalingGroups	Concede permiso para enumerar los grupos de escalado en un entorno de kdb administrado	Enumeración	kxEnvironment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListKxUsers	Concede permiso para enumerar los usuarios en un entorno de kdb administrado	Enumeración	kxEnvironment*		
ListKxVolumes	Concede permiso para enumerar los volúmenes en un entorno de kdb administrado	Enumeración	kxEnvironment*		
ListTagsForResource	Concede permiso para devolver una lista de etiquetas de un recurso	Enumeración	environment*		
			kxCluster*		
			kxDatabase*		
			kxDataview*		
			kxEnvironment*		
			kxScalingGroup*		
			kxUser*		
			kxVolume*		
ListUsers	Otorga permiso para incluir FinSpace usuarios en un entorno	Enumeración	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			user*		
LoadSampleDataSetGroupIntoEnvironment	Otorga permiso para cargar un paquete de datos de muestra en su FinSpace entorno	Escritura	environment*		
MountKxDatabase [solo permiso]	Concede permiso para montar una base de datos en un clúster de kdb	Escritura	kxDatabase*		
ResetUserPassword	Otorga permiso para restablecer la contraseña de un FinSpace usuario	Escritura	environment*		
			user*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			kxVolume		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys	
UpdateEnvironment	Otorga permiso para actualizar un FinSpace entorno	Escritura	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateKxClusterCodeConfiguration	Concede permiso para actualizar la configuración del código para un clúster en un entorno de kdb administrado	Escritura	kxCluster*		
UpdateKxClusterDatabases	Concede permiso para actualizar las bases de datos de un clúster en un entorno de kdb administrado	Escritura	kxCluster*		
UpdateKxDatabase	Concede permiso para actualizar una base de datos de kdb	Escritura	kxDatabase*		
UpdateKxDataview	Concede permiso para actualizar una vista de datos en un entorno de kdb administrado	Escritura	kxDataview*		
UpdateKxEnvironment	Concede permiso para actualizar un entorno de kdb administrado	Escritura	kxEnvironment*		
UpdateKxEnvironmentNetwork	Concede permiso para actualizar la red para un entorno de kdb administrado	Escritura	kxEnvironment*		
UpdateKxUser	Concede permiso para actualizar un usuario de kdb	Escritura	kxUser*		
UpdateKxVolume	Concede permiso para actualizar un volumen en un entorno de kdb administrado	Escritura	kxVolume*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateUser	Otorga permiso para actualizar a un FinSpace usuario	Escritura	environment*		
			user*		

Tipos de recursos definidos por Amazon FinSpace

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment	`arn:${Partition}:finspace:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:finspace:${Region}:${Account}:user/${UserId}`	aws:ResourceTag/${TagKey}
kxEnvironment	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
kxUser	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxUser/${UserName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
kxCluster	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxCluster/${KxCluster}`	aws:ResourceTag/${TagKey}
kxDatabase	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}`	aws:ResourceTag/${TagKey}
kxScalingGroup	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxScalingGroup/${KxScalingGroup}`	aws:ResourceTag/${TagKey}
kxDataview	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}/kxDataview/${KxDataview}`	aws:ResourceTag/${TagKey}
kxVolume	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxVolume/${KxVolume}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon FinSpace

Amazon FinSpace define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de la FinSpace API de Amazon

La FinSpace API de Amazon (prefijo de servicio:`finspace-api`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la FinSpace API de Amazon
- Tipos de recursos definidos por la FinSpace API de Amazon
- Claves de condición para la FinSpace API de Amazon

Acciones definidas por la FinSpace API de Amazon

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetProgrammaticAccessCredentials	Otorga permiso para recuperar las credenciales de FinSpace acceso programático	Lectura	credential*		

Tipos de recursos definidos por la FinSpace API de Amazon

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
credential	`arn:${Partition}:finspace-api:${Region}:${Account}:/credentials/programmatic`	

Claves de condición para la FinSpace API de Amazon

FinSpace La API no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Firewall Manager

AWS Firewall Manager (prefijo de servicio:`fms`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Firewall Manager
- Tipos de recursos definidos por AWS Firewall Manager
- Claves de condición para AWS Firewall Manager

Acciones definidas por AWS Firewall Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateAdminAccount	Otorga permiso para configurar la cuenta de administrador del AWS Firewall Manager y habilita el servicio en todas las cuentas de la organización	Escritura			
AssociateThirdPartyFirewall	Otorga permiso para configurar al administrador de Firewall Manager como administrador	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de inquilinos de un servicio de firewall de terceros				
BatchAssociateResource	Otorga permiso para asociar recursos a un conjunto de recursos del AWS Firewall Manager	Escritura	resource-set*		
BatchDisassociateResource	Otorga permiso para desasociar recursos de un conjunto de recursos del AWS Firewall Manager	Escritura	resource-set*		
DeleteAppsList	Otorga permiso para eliminar permanentemente una lista de aplicaciones AWS del Firewall Manager	Escritura	applications-list*		
DeleteNotificationChannel	Otorga permiso para eliminar una asociación de AWS Firewall Manager con la función de IAM y el tema Amazon Simple Notification Service (SNS) que se utiliza para notificar al administrador de FM sobre los principales eventos y errores de FM en la organización	Escritura			
DeletePolicy	Otorga permiso para eliminar permanentemente una política de AWS Firewall Manager	Escritura	policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeleteProtocolsList	Otorga permiso para eliminar permanentemente una lista de protocolos AWS del Firewall Manager	Escritura	protocols-list*		
DeleteResourceSet	Otorga permiso para eliminar permanentemente un conjunto de recursos del AWS Firewall Manager	Escritura	resource-set*		
				aws:ResourceTag/${TagKey}	
DisassociateAdminAccount	Otorga permiso para desasociar la cuenta que se ha establecido como cuenta de administrador del AWS Firewall Manager y desactiva el servicio en todas las cuentas de la organización.	Escritura			
DisassociateThirdPartyFirewall	Concede permiso para disociar un administrador de Firewall Manager de un inquilino de firewall de terceros	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAdminAccount	Otorga permiso para devolver la AWS cuenta de la Organización que está asociada a AWS Firewall Manager como administrador de AWS Firewall Manager	Lectura			
GetAdminScope	Concede permiso para devolver información sobre el ámbito administrativo de la cuenta especificada	Lectura			
GetAppsList	Otorga permiso para devolver información sobre la lista de aplicaciones del AWS Firewall Manager especificada	Lectura	applications-list*		
GetComplianceDetail	Otorga permiso para recuperar información de conformidad detallada acerca de la cuenta miembro especificada. En los detalles se incluyen recursos que cumplen y no cumplen la política especificada.	Lectura	policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetNotificationChannel	Otorga permiso para recuperar información sobre el tema Amazon Simple Notification Service (SNS) que se utiliza para registrar los registros de SNS de Firewall Manager AWS	Lectura			
GetPolicy	Otorga permiso para recuperar información sobre la política de AWS Firewall Manager especificada	Lectura	policy*		
GetProtectionStatus	Otorga permiso para recuperar información resumida sobre los ataques a nivel de política en caso de que se produzca un posible DDo ataque S	Lectura	policy*		
GetProtocolsList	Otorga permiso para devolver información sobre la lista de protocolos del AWS Firewall Manager especificada	Lectura	protocols-list*		
GetResourceSet	Otorga permiso para recuperar información sobre el conjunto de recursos del AWS Firewall Manager especificado	Lectura	resource-set*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetThirdPartyFirewallAssociationStatus	Otorga permiso para recuperar el estado de incorporación de una cuenta de administrador de Firewall Manager a un inquilino de proveedor de firewall de terceros	Lectura			
GetViolationDetails	Otorga permiso para recuperar las infracciones de un recurso en función de la política de AWS Firewall Manager especificada y Cuenta de AWS	Lectura	policy*		
ListAdminAccountsForOrganization	Otorga permiso para devolver un AdminAccounts objeto en el que se enumeran los administradores del Firewall Manager de la organización que han sido incorporados a Firewall Manager por AssociateAdminAccount	Enumeración			
ListAdminsManagingAccount	Otorga permiso para enumerar las cuentas que administran la cuenta de miembro de AWS Organizations especificada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAppsLists	Otorga permiso para devolver una matriz de AppsListDataSummary objetos	Enumeración			
ListComplianceStatus	Otorga permiso para recuperar una matriz de PolicyComplianceStatus objetos de la respuesta. Se utiliza PolicyComplianceStatus para obtener un resumen de las cuentas de los miembros que están protegidas por la política especificada	Enumeración	policy*		
ListDiscoveredResources	Otorga permiso para recuperar una matriz de recursos de las cuentas de la organización que están disponibles para asociarse a un conjunto de recursos	Enumeración			
ListMemberAccounts	Otorga permiso para recuperar una matriz de ID de cuentas miembro si el llamante es una cuenta de administrador de FMS.	Enumeración			
ListPolicies	Otorga permiso para recuperar una matriz de PolicySummary objetos de la respuesta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProtocolsLists	Otorga permiso para devolver una matriz de Protocols ListDataSummary objetos	Enumeración			
ListResourceSetResources	Otorga permiso para recuperar una matriz de recursos que están asociados actualmente a un conjunto de recursos	Enumeración	resource-set*		
ListResourceSets	Otorga permiso para recuperar una matriz de ResourceSetSummary objetos	Enumeración			
ListTagsForResource	Otorga permiso para mostrar una lista de etiquetas de un recurso determinado.	Lectura	policy*		
ListThirdPartyFirewallFirewallPolicies	Otorga permiso para recuperar una lista de todas las políticas de firewall de terceros asociadas a la cuenta del administrador del firewall de terceros	Enumeración			
PutAdminAccount	Concede permiso para crear o actualizar una cuenta de administrador de Firewall Manager	Escritura			
PutAppsList	Otorga permiso para crear una lista de aplicaciones del AWS Firewall Manager	Escritura	applications-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
PutNotificationChannel	Otorga permiso para designar la función de IAM y el tema de Amazon Simple Notification Service (SNS) que AWS Firewall Manager (FM) podría utilizar para notificar al administrador de FM sobre los principales eventos y errores de FM en la organización	Escritura			
PutPolicy	Otorga permiso para crear una política de AWS Firewall Manager	Escritura	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutProtocolsList	Otorga permiso para crear una lista de protocolos del AWS Firewall Manager	Escritura	protocols-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
PutResourceSet	Otorga permiso para crear un conjunto de recursos de AWS Firewall Manager	Escritura	resource-set*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Otorga permiso para agregar una etiqueta a un recurso determinado.	Etiquetado	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso determinado.	Etiquetado	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:TagKeys	

Tipos de recursos definidos por AWS Firewall Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
policy	`arn:${Partition}:fms:${Region}:${Account}:policy/${Id}`	aws:ResourceTag/${TagKey}
applications-list	`arn:${Partition}:fms:${Region}:${Account}:applications-list/${Id}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
protocols-list	`arn:${Partition}:fms:${Region}:${Account}:protocols-list/${Id}`	aws:ResourceTag/${TagKey}
resource-set	`arn:${Partition}:fms:${Region}:${Account}:resource-set/${Id}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Firewall Manager

AWS Firewall Manager define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Forecast

Amazon Forecast (prefijo de servicio: `forecast`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Forecast
- Tipos de recurso definidos por Amazon Forecast
- Claves de condición de Amazon Forecast

Acciones definidas por Amazon Forecast

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAutoPredictor	Concede permiso para crear un predictor automático.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Concede permiso para crear un conjunto de datos	Write	dataset*	aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDatasetGroup	Concede permiso para crear un grupo de conjuntos de datos.	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetImportJob	Concede permiso para crear un trabajo de importación de conjuntos de datos	Escritura	datasetImportJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainability	Concede permiso para crear una explicabilidad.	Escritura	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainabilityExport	Concede permiso para crear una exportación de explicabilidad mediante un recurso de explicabilidad.	Escritura	explainability*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecast	Concede permiso para crear una predicción	Escritura	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastEndpoint [solo permiso]	Concede permiso para crear un punto de conexión mediante un recurso Predictor	Escritura	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastExportJob	Concede permiso para crear un trabajo de exportación de predicciones utilizando un recurso de predicción	Escritura	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMonitor	Concede permiso para crear un monitor mediante un recurso Predictor	Escritura	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictor	Concede permiso para crear un predictor	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictorBacktestExportJob	Concede permiso para crear un trabajo de exportación de pruebas sobre datos históricos utilizando un predictor	Escritura	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfAnalysis	Concede permiso para crear un análisis de hipótesis	Escritura	forecast*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecast	Concede permiso para crear una previsión de hipótesis	Escritura	whatIfAnalysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecastExport	Concede permiso para crear una exportación de previsiones de hipótesis mediante recursos de previsión de hipótesis	Escritura	whatIfForecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Concede permiso para eliminar un conjunto de datos	Write	dataset*		
DeleteDatasetGroup	Concede permiso para eliminar un grupo de conjuntos de datos	Write	datasetGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDatasetImportJob	Concede permiso para eliminar un trabajo de importación de conjuntos de datos	Escritura	datasetImportJob*		
DeleteExplainability	Concede permiso para eliminar una explicabilidad.	Escritura	explainability*		
DeleteExplainabilityExport	Concede permiso para eliminar una exportación de explicabilidad.	Escritura	explainabilityExport*		
DeleteForecast	Concede permiso para eliminar una predicción	Escritura	forecast*		
DeleteForecastEndpoint [solo permiso]	Concede permiso para eliminar un punto de conexión.	Escritura	endpoint*		
DeleteForecastExportJob	Concede permiso para eliminar un trabajo de exportación de predicciones	Escritura	forecastExport*		
DeleteMonitor	Concede permiso para eliminar un recurso de monitor	Escritura	monitor*		
DeletePredictor	Concede permiso para eliminar un predictor	Write	predictor*		
DeletePredictorBacktestExportJob	Concede permiso para eliminar un trabajo de exportación de pruebas sobre datos históricos de predictor	Write	predictorBacktestExportJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourceTree	Concede permiso para eliminar un recurso y sus recursos secundarios	Escritura	dataset*		
			datasetGroup*		
			datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			whatIfForecastExport*		
DeleteWhatIfAnalysis	Concede permiso para eliminar un análisis de hipótesis	Escritura	whatIfAnalysis*		
DeleteWhatIfForecast	Concede permiso para eliminar una previsión de hipótesis	Escritura	whatIfForecast*		
DeleteWhatIfForecastExport	Concede permiso para eliminar una exportación de previsiones de hipótesis	Escritura	whatIfForecastExport*		
DescribeAutoPredictor	Concede permiso para describir un predictor automático.	Lectura	predictor*		
DescribeDataset	Concede permiso para describir un conjunto de datos	Read	dataset*		
DescribeDatasetGroup	Concede permiso para describir un grupo de conjuntos de datos	Read	datasetGroup*		
DescribeDatasetImportJob	Concede permiso para describir un trabajo de importación de conjuntos de datos	Lectura	datasetImportJob*		
DescribeExplainability	Concede permiso para describir una explicabilidad.	Lectura	explainability*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeExplainabilityExport	Concede permiso para describir una exportación de explicabilidad.	Lectura	explainabilityExport*		
DescribeForecast	Concede permiso para describir una predicción	Lectura	forecast*		
DescribeForecastEndpoint [solo permiso]	Concede permiso para describir un recurso de punto de conexión	Lectura	endpoint*		
DescribeForecastExportJob	Concede permiso para describir un trabajo de exportación de predicciones	Lectura	forecastExport*		
DescribeMonitor	Concede permiso para describir un recurso de monitor	Lectura	monitor*		
DescribePredictor	Concede permiso para describir un predictor	Read	predictor*		
DescribePredictorBacktestExportJob	Concede permiso para describir un trabajo de exportación de pruebas sobre datos históricos de predictor	Lectura	predictorBacktestExportJob*		
DescribeWhatIfAnalysis	Concede permiso para describir un análisis de hipótesis	Lectura	whatIfAnalysis*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeWhatIfForecast	Concede permiso para describir una previsión de hipótesis	Lectura	whatIfForecast*		
DescribeWhatIfForecastExport	Concede permiso para describir una exportación de previsiones de hipótesis	Lectura	whatIfForecastExport*		
GetAccuracyMetrics	Concede permiso para obtener las métricas de precisión de un predictor	Lectura	predictor*		
GetRecentForecastContext [solo permiso]	Concede permiso para obtener el contexto de previsión de una serie temporal de un punto de conexión	Lectura	endpoint*		
InvokeForecastEndpoint [solo permiso]	Concede permiso para invocar el punto de conexión a fin de obtener la previsión de una serie temporal	Lectura	endpoint*		
ListDatasetGroups	Concede permiso para enumerar todos los grupos de conjuntos de datos	Lectura			
ListDatasetImportJobs	Concede permiso para enumerar todos los trabajos de importación de conjuntos de datos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDatasets	Concede permiso para enumerar todos los conjuntos de datos	Lectura			
ListExplainabilities	Concede permiso para enumerar todas las explicabilidades.	Lectura			
ListExplainabilityExports	Concede permiso para enumerar todas las exportaciones de explicabilidad.	Lectura			
ListForecastExportJobs	Concede permiso para enumerar todos los trabajos de exportación de predicciones	Lectura			
ListForecasts	Concede permiso para enumerar todas las predicciones	Lectura			
ListMonitorEvaluations	Concede permiso para enumerar todos los resultados de evaluación de un monitor	Lectura	monitor*		
ListMonitors	Concede permiso para enumerar todos los recursos de monitor	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPredictorBacktestExportJobs	Concede permiso para enumerar todos los trabajos de exportación de pruebas sobre datos históricos de predictor	Lectura			
ListPredictors	Concede permiso para enumerar todos los predictores	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso de Amazon Forecast	Lectura	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
ListWhatIfAnalyses	Concede permiso para enumerar todos los análisis de hipótesis	Lectura			
ListWhatIfForecastExports	Concede permiso para enumerar todas las exportaciones de previsiones de hipótesis	Lectura			
ListWhatIfForecasts	Concede permiso para enumerar todas las previsiones de hipótesis	Lectura			
QueryForecast	Concede permiso para recuperar una predicción de un solo elemento	Lectura	forecast*		
QueryWhatIfForecast	Concede permiso para recuperar una previsión de hipótesis de un solo elemento	Lectura	whatIfForecast*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResumeResource	Concede permiso para reanudar trabajos de recursos de Amazon Forecast	Escritura	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopResource	Concede permiso para detener trabajos de recursos de Amazon Forecast.	Write	datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para asociar las etiquetas especificadas a un recurso	Etiquetado	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas especificadas de un recurso	Etiquetado	dataset		
			datasetGroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateDatasetGroup	Concede permiso para actualizar un grupo de conjuntos de datos	Write	dataset*		
			datasetGroup*		

Tipos de recurso definidos por Amazon Forecast

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
dataset	`arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
datasetGroup	`arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}`	aws:ResourceTag/${TagKey}
datasetImportJob	`arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
algorithm	arn:${Partition}:forecast:::algorithm/${ResourceId}	
predictor	arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}	aws:ResourceTag/${TagKey}
predictorBacktestExportJob	arn:${Partition}:forecast:${Region}:${Account}:predictor-backtest-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
forecast	arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}	aws:ResourceTag/${TagKey}
forecastExport	arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
explainability	arn:${Partition}:forecast:${Region}:${Account}:explainability/${ResourceId}	aws:ResourceTag/${TagKey}
explainabilityExport	arn:${Partition}:forecast:${Region}:${Account}:explainability-export/${ResourceId}	aws:ResourceTag/${TagKey}
monitor	arn:${Partition}:forecast:${Region}:${Account}:monitor/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfAnalysis	arn:${Partition}:forecast:${Region}:${Account}:what-if-analysis/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfForecast	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast/${ResourceId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
whatIfForecastExport	`arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast-export/${ResourceId}`	aws:ResourceTag/${TagKey}
endpoint	`arn:${Partition}:forecast:${Region}:${Account}:forecast-endpoint/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Forecast

Amazon Forecast define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Fraud Detector

Amazon Fraud Detector (prefijo de servicio: `frauddetector`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Fraud Detector
- Tipos de recursos definidos por Amazon Fraud Detector
- Claves de condición para Amazon Fraud Detector

Acciones definidas por Amazon Fraud Detector

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchCreateVariable	Otorga permiso para crear un lote de variables	Write		aws:RequestTag/${TagKey} aws:TagKeys	
BatchGetVariable	Otorga permiso para obtener un lote de variables	Enumeración	variable*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelBatchImportJob	Otorga el permiso para cancelar el trabajo de importación de lotes especificado	Escritura	batch-import*		
CancelBatchPredictionJob	Otorga permiso para cancelar el trabajo de predicción de lotes especificado	Escritura	batch-prediction*		
CreateBatchImportJob	Otorga el permiso para crear un trabajo de importación de lotes	Escritura	batch-import*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBatchPredictionJob	Otorga permiso para crear un trabajo de predicción por lotes	Write	batch-prediction*		
			detector*		
			detector-version*		
			event-type*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorVersion	Otorga permiso para crear una versión de detector. La versión de detector comienza con el estado BORRADOR	Escritura	detector*		
			external-model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateList	Otorga permiso para crear una lista	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Otorga permiso para crear un modelo con el tipo de modelo especificado	Write	event-type*		
			model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelVersion	Otorga permiso para crear una versión del modelo con el tipo de modelo y el ID de modelo especificados	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRule	Otorga permiso para crear una regla para su uso con el detector especificado	Write	detector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVariable	Otorga permiso para crear una variable	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBatchImportJob	Otorga el permiso para eliminar un trabajo de importación de lotes	Escritura	batch-import*		
DeleteBatchPredictionJob	Otorga permiso para eliminar un trabajo de predicción por lotes	Write	batch-prediction*		
DeleteDetector	Otorga permiso para eliminar el detector. Antes de eliminar un detector, primero debe eliminar todas las versiones del detector y las versiones de reglas asociadas al detector.	Write	detector*		
DeleteDetectorVersion	Otorga permiso para eliminar la versión del detector. No se pueden eliminar las versiones del detector que estén en estado ACTIVO	Write	detector-version*		
DeleteEntityType	Otorga permiso para eliminar un tipo de entidad. No se puede eliminar un tipo de entidad incluido en un tipo de evento	Write	entity-type*		
DeleteEvent	Otorga permiso para eliminar el evento especificado	Write	event-type*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEventType	Otorga permiso para eliminar un tipo de evento. No se puede eliminar un tipo de evento que se utiliza en un detector o modelo	Escritura	event-type*		
DeleteEventsByEventType	Otorga el permiso para eliminar eventos para el tipo evento especificado	Escritura	event-type*		
DeleteExternalModel	Concede permiso para eliminar un SageMaker modelo de Amazon Fraud Detector. Puedes eliminar un SageMaker modelo de Amazon si no está asociado a una versión de detector	Escritura	external-model*		
DeleteLabel	Otorga permiso para eliminar una etiqueta. No puede eliminar etiquetas incluidas en un tipo de evento en Amazon Fraud Detector. No se puede eliminar una etiqueta asignada a un identificador de evento. Primero debe eliminar el ID de evento relevante	Escritura	label*		
DeleteList	Otorga permiso para eliminar una lista	Escritura	list*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteModel	Otorga permiso para eliminar un modelo. Puede eliminar modelos y versiones de modelo en Amazon Fraud Detector, siempre que no estén asociados a una versión de detector	Write	model*		
DeleteModelVersion	Otorga permiso para eliminar una versión de modelo. Puede eliminar modelos y versiones de modelo en Amazon Fraud Detector, siempre que no estén asociados a una versión de detector	Write	model-version*		
DeleteOutcome	Otorga permiso para eliminar un resultado. No se puede eliminar un resultado que se utiliza en una versión de regla	Write	outcome*		
DeleteRule	Otorga permiso para eliminar la regla. No se puede eliminar una regla si la utiliza una versión de detector ACTIVO o INACTIVO	Write	rule*		
DeleteVariable	Otorga permiso para eliminar una variable. No puede eliminar variables incluidas en un tipo de evento en Amazon Fraud Detector	Write	variable*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDetector	Otorga permiso para obtener todas las versiones de un detector especificado	Read	detector*		
DescribeModelVersions	Otorga permiso para obtener todas las versiones de modelo para el tipo de modelo especificado o el tipo de modelo y el ID de modelo especificados. También puede obtener detalles de una sola versión de modelo especificada	Lectura	model-version		
GetBatchImportJobValidationReport [solo permiso]	Concede permiso para obtener el informe de validación de datos de un trabajo de importación de lotes específico	Lectura	batch-import*		
GetBatchImportJobs	Otorga el permiso para obtener todos los trabajos de importación de lotes o un trabajo específico si especifica un ID de trabajo.	Enumeración	batch-import		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBatchPredictionJobs	Otorga permiso para obtener todos los trabajos de predicción por lotes o un trabajo específico si especifica un ID de trabajo. Esta es una API paginada. Si proporciona un valor maxResults nulo, esta acción recupera un máximo de 50 registros por página. Si proporciona un valor maxResults, el valor debe estar entre 1 y 50. Para obtener los resultados de la página siguiente, proporciona el token de paginación de GetBatchPredictionJobsResponse como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	Enumeración	batch-prediction		
GetDeleteEventsByEventTypeStatus	Otorga permiso para obtener el estado de ejecución de la DeleteEventsByEventType API de un tipo de evento específico	Lectura	event-type*		
GetDetectorVersion	Otorga permiso para obtener una versión de detector en particular	Lectura	detector-version*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDetectors	Otorga permiso para obtener todos los detectores o uno solo si se especifica un detectorId. Esta es una API paginada. Si proporciona un maxResults nulo, esta acción recupera un máximo de 10 registros por página. Si proporciona un maxResults, el valor debe estar entre 5 y 10. Para obtener los resultados de la página siguiente, proporciona el token de paginación de GetDetectorsResponse como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	List	detector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEntityTypes	Otorga permiso para obtener todos los tipos de entidad o un tipo de entidad específico o si se especifica un nombre. Esta es una API paginada. Si proporciona un maxResults nulo, esta acción recupera un máximo de 10 registros por página. Si proporciona un maxResults, el valor debe estar entre 5 y 10. Para obtener los resultados de la página siguiente, proporciona el token de paginación de GetEntityTypesResponse como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	Enumeración	entity-type		
GetEvent	Otorga el permiso para obtener los detalles del evento especificado	Lectura	event-type*		
GetEventPrediction	Otorga permiso para evaluar un evento en relación con una versión de detector. Si no se proporciona un ID de versión, se utiliza la versión (ACTIVA) del detector	Lectura	detector*		
			detector-version*		
			event-type*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEventPrediction Metadata	Otorga permiso para obtener más detalles de una predicción en particular	Lectura	detector*		
			detector-version*		
			event-type*		
GetEventTypes	Otorga permiso para obtener todos los tipos de evento o un tipo de evento específico si se proporciona un nombre. Esta es una API paginada. Si proporciona un maxResults nulo, esta acción recupera un máximo de 10 registros por página. Si proporciona un maxResults, el valor debe estar entre 5 y 10. Para obtener los resultados de la página siguiente, proporciona el token de paginación de GetEventTypesResponse como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	Enumeración	event-type		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetExternalModels	Otorga permiso para obtener los detalles de uno o más SageMaker modelos de Amazon que se han importado al servicio. Esta es una API paginada. Si proporciona un valor maxResults nulo, esta acción obtendrá un máximo de 10 registros por página. Si proporciona un maxResults, el valor debe estar entre 5 y 10. Para obtener los resultados de la página siguiente, proporciona el token de paginación de GetExternalModelsResult como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	List	external-model		
GetKMSEncryptionKey	Otorga permiso para obtener la clave de cifrado si se ha especificado una clave maestra de cliente (CMK) de Key Management Service (KMS) a fin de que se utilice para cifrar contenido en Amazon Fraud Detector	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLabels	Otorga permiso para obtener todas las etiquetas o una etiqueta específica si se proporciona un nombre. Esta es una API paginada. Si proporciona un valor maxResults nulo, esta acción recupera un máximo de 50 registros por página. Si proporciona un valor maxResults, el valor debe estar entre 10 y 50. Para obtener los resultados de la página siguiente, proporcio na el token de paginación de GetGetLabelsResponse como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	Enumeración	label		
GetListElements	Otorga permiso para obtener elementos de una lista	Lectura	list*		
				aws:ResourceTag/${TagKey}	
GetListsMetadata	Otorga permiso para obtener metadatos de las listas	Enumeración	list		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetModelVersion	Otorga permiso para obtener los detalles de la versión del modelo especificada	Lectura	model-version*		
GetModels	Otorga permiso para obtener uno o más modelos. Obtiene todos los modelos Cuenta de AWS si no se ha proporcionado ningún tipo de modelo ni identificador de modelo. Obtiene todos los modelos del tipo de modelo Cuenta de AWS y, si se especifica el tipo de modelo pero no se proporciona el identificador del modelo. Obtiene un modelo específico si se especifica una tupla (tipo de modelo, ID de modelo)	List	model		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOutcomes	Otorga permiso para obtener uno o más resultados. Esta es una API paginada. Si proporciona un valor MaxSizePerPage nulo, esta acción obtendrá un máximo de 100 registros por página. Si proporciona un valor maxResults, el valor debe estar entre 50 y 100. Para obtener los resultados de la página siguiente, proporcio na el token de paginación de GetOutcomesResult como parte de tu solicitud. Un token de paginación nulo obtiene los registros desde el principio	List	outcome		
GetRules	Otorga permiso para obtener todas las reglas de un detector (paginado) si no se especific an ruleId y ruleVersion. Obtiene todas las reglas para el detector y el ruleId si están presentes (paginado). Obtiene una regla específica si se especifican tanto ruleId como ruleVersion	List	rule		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVariables	Otorga permiso para obtener todas las variables o la variable específica. Esta es una API paginada. Si se proporciona una maxSizePer página nula, se recuperarán un máximo de 100 registros por página. Si proporciona maxSizePer Page, el valor debe estar entre 50 y 100. Para obtener el resultado de la página siguiente, proporciona un token de paginación GetVariablesResult como parte de tu solicitud. El token de paginación nulo obtiene los registros desde el principio	Enumeración	variable		
ListEvent Predictions	Otorga permiso para obtener una lista de predicciones anteriores	Enumeración	detector		
			detector-version		
			event-type		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para mostrar todas las etiquetas asociadas al recurso. Esta es una API paginada. Para obtener los resultados de la página siguiente, proporcione el token de paginación de GetEventTypesResponse como parte de su solicitud. Un token de paginación nulo obtiene los registros desde el principio	Lectura	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutDetector	Otorga permiso para crear o actualizar un detector	Write	detector*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutEntityType	Otorga permiso para crear o actualizar un tipo de entidad. Una entidad representa quién está realizando el evento. Como parte de una predicción de fraude, se pasa el ID de entidad para indicar la entidad específica que realizó el evento. Un tipo de entidad clasifica la entidad. Entre las clasificaciones de ejemplo se incluyen cliente, comerciante o cuenta	Write	entity-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutEventType	Otorga permiso para crear o actualizar un tipo de evento. Un evento es una actividad empresarial que se evalúa para detectar el riesgo de fraude. Con Amazon Fraud Detector, genere predicciones de fraude para eventos. Un tipo de evento define la estructura de un evento enviado a Amazon Fraud Detector. Esto incluye las variables enviadas como parte del evento, la entidad que realiza el evento (como un cliente) y las etiquetas que clasifican el evento. Los tipos de eventos de ejemplo incluyen transacciones de pago en línea, registros de cuentas y autenticaciones	Escritura	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutExternalModel	Otorga permiso para crear o actualizar un dispositivo de punto final de un SageMaker modelo de Amazon. También puede utilizar esta acción para actualizar la configuración del punto final del modelo, incluida la función and/or de IAM y las variables mapeadas	Escritura	event-type*		
			external-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutKMSEncryptionKey	Otorga permiso para especificar la clave maestra de cliente (CMK) de Key Management Service (KMS) que se utilizará a fin de cifrar contenido en Amazon Fraud Detector	Write			
PutLabel	Otorga permiso para crear o actualizar la etiqueta. Una etiqueta clasifica un evento como fraudulento o legítimo. Las etiquetas se asocian a tipos de eventos y se utilizan para entrenar modelos de Machine Learning supervisados en Amazon Fraud Detector	Write	label*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutOutcome	Otorga permiso para crear o actualizar un resultado	Escritura	outcome*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
SendEvent	Otorga el permiso para enviar el evento	Escritura	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Otorga permiso para asignar etiquetas a un recurso	Etiquetado	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	batch-import		
			batch-prediction		
			detector		
			detector-version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDetectorVersion	Otorga permiso para actualizar una versión del detector. Los atributos de la versión del detector que se pueden actualizar incluyen modelos, puntos de enlace externos del modelo, normas, modo de ejecución de normas y descripción. Solo se puede actualizar una versión del detector que sea BORRADOR	Write	detector*		
			external-model		
			model-version		
UpdateDetectorVersionMetadata	Otorga permiso para actualizar la descripción de la versión del detector. Puede actualizar los metadatos de cualquier versión del detector (BORRADOR, ACTIVO o INACTIVO)	Escritura	detector-version*		
UpdateDetectorVersionStatus	Concede permiso para actualizar el estado de la versión del detector. Puede realizar los siguientes ascensos o descensos de categoría utilizando UpdateDetectorVersionStatus: DRAFT a ACTIVO, ACTIVO a INACTIVO e INACTIVO a ACTIVO	Escritura	detector-version*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEventLabel	Otorga el permiso para actualizar el valor de etiqueta de un registro de evento existente	Escritura	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateList	Otorga permiso para actualizar una lista	Escritura	list*		
				aws:ResourceTag/${TagKey}	
UpdateModel	Otorga permiso para actualizar un modelo. Puede actualizar el atributo de descripción mediante esta acción	Write	model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateModelVersion	Otorga permiso para actualizar una versión de modelo. La actualización de una versión de modelo vuelve a entrenar una versión de modelo existente utilizando datos de formación actualizados y genera una nueva versión secundaria del modelo. Puede actualizar los atributos de ubicación y función de acceso del conjunto de datos de formación mediante esta acción. Esta acción crea y entrena una nueva versión secundaria del modelo; por ejemplo, la versión 1.01, 1.02, 1.03	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateModelVersionStatus	Otorga permiso para actualizar el estado de una versión de modelo	Write	model-version*		
UpdateRuleMetadata	Otorga permiso para actualizar los metadatos de una regla. Se puede actualizar el atributo de descripción	Write	rule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRuleVersion	Otorga permiso para actualizar una versión de regla que da como resultado una versión de regla nueva. Actualiza una versión de regla que da como resultado una versión de regla nueva (versión 1, 2, 3...)	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVariable	Otorga permiso para actualizar una variable	Write	variable*		

Tipos de recursos definidos por Amazon Fraud Detector

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
batch-prediction	`arn:${Partition}:frauddetector:${Region}:${Account}:batch-prediction/${ResourcePath}`	aws:ResourceTag/${TagKey}
detector	`arn:${Partition}:frauddetector:${Region}:${Account}:detector/${ResourcePath}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
detector-version	arn:${Partition}:frauddetector:${Region}:${Account}:detector-version/${ResourcePath}	aws:ResourceTag/${TagKey}
entity-type	arn:${Partition}:frauddetector:${Region}:${Account}:entity-type/${ResourcePath}	aws:ResourceTag/${TagKey}
external-model	arn:${Partition}:frauddetector:${Region}:${Account}:external-model/${ResourcePath}	aws:ResourceTag/${TagKey}
event-type	arn:${Partition}:frauddetector:${Region}:${Account}:event-type/${ResourcePath}	aws:ResourceTag/${TagKey}
label	arn:${Partition}:frauddetector:${Region}:${Account}:label/${ResourcePath}	aws:ResourceTag/${TagKey}
model	arn:${Partition}:frauddetector:${Region}:${Account}:model/${ResourcePath}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:frauddetector:${Region}:${Account}:model-version/${ResourcePath}	aws:ResourceTag/${TagKey}
outcome	arn:${Partition}:frauddetector:${Region}:${Account}:outcome/${ResourcePath}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:frauddetector:${Region}:${Account}:rule/${ResourcePath}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
variable	`arn:${Partition}:frauddetector:${Region}:${Account}:variable/${ResourcePath}`	aws:ResourceTag/${TagKey}
batch-import	`arn:${Partition}:frauddetector:${Region}:${Account}:batch-import/${ResourcePath}`	aws:ResourceTag/${TagKey}
list	`arn:${Partition}:frauddetector:${Region}:${Account}:list/${ResourcePath}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Fraud Detector

Amazon Fraud Detector define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso.	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el nivel gratuito de AWS

AWS Free Tier (prefijo de servicio:`freetier`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el nivel gratuito de AWS
- Tipos de recursos definidos por el nivel gratuito de AWS
- Claves de condición para el nivel gratuito de AWS

Acciones definidas por el nivel gratuito de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFreeTierAlertPreference [solo permiso]	Otorga permiso para obtener una preferencia de alerta de nivel gratuito (dirección de correo electrónico)	Lectura			
GetFreeTierUsage	Otorga permiso para obtener los límites de uso del nivel gratuito y el estado de uso del mes hasta la fecha (MTD)	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutFreeTierAlertPreference [solo permiso]	Otorga permiso para establecer una preferencia de alerta de nivel gratuito (dirección de correo electrónico)	Escritura			

Tipos de recursos definidos por el nivel gratuito de AWS

AWS Free Tier no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al nivel gratuito de AWS , especifique `"Resource": "*"` en la política.

Claves de condición para el nivel gratuito de AWS

El nivel gratuito no tiene claves de contexto específicas del servicio que puedan utilizarse en el elemento `Condition` de las instrucciones de políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon FreeRTOS

Amazon FreeRTOS (prefijo de servicio: `freertos`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon FreeRTOS
- Tipos de recursos definidos por Amazon FreeRTOS
- Claves de condición para Amazon FreeRTOS

Acciones definidas por Amazon FreeRTOS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSoftwareConfiguration	Concede permiso para crear una configuración de software	Escritura	configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Concede permiso para crear una suscripción para el plan de mantenimiento extendido (EMP) de FreeRTOS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSoftwareConfiguration	Concede permiso para eliminar la configuración de software	Escritura	configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeHardwarePlatform	Concede permiso para describir la plataforma de hardware	Lectura			
DescribeSoftwareConfiguration	Concede permiso para describir la configuración de software	Lectura	configuration*		
DescribeSubscription	Concede permiso para describir la suscripción para el plan de mantenimiento extendido (EMP) de FreeRTOS	Lectura	subscription*		
GetEmpPatchUrl	Concede permiso para obtener la URL de la versión del parche, la diferencia del parche y las notas de la versión del software en virtud del plan de mantenimiento extendido (EMP) de FreeRTOS	Lectura			
GetSoftwareURL	Concede permiso para obtener la URL para la descarga del software Amazon FreeRTOS	Lectura			
GetSoftwareURLForConfiguration	Concede permiso para obtener la URL para la descarga del software Amazon FreeRTOS en función de la configuración	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSubscriptionBillingAmount	Concede permiso para recuperar el importe de facturación de la suscripción para el plan de mantenimiento extendido (EMP) de FreeRTOS	Lectura			
ListFreeRTOSVersions	Otorga permiso para enumerar versiones de RTOS AmazonFree	Enumeración			
ListHardwarePlatforms	Concede permiso para enumerar las plataforma de hardware	Enumeración			
ListHardwareVendors	Concede permiso para enumerar los proveedores de hardware	Enumeración			
ListSoftwareConfigurations	Concede permiso para enumerar la configuración de software	Enumeración			
ListSoftwarePatches	Concede permiso para enumerar los parches del software de la suscripción para el plan de mantenimiento extendido (EMP) de FreeRTOS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSubscriptionEmails	Concede permiso para enumerar los correos electrónicos de suscripción para el plan de mantenimiento extendido (EMP) de FreeRTOS	Enumeración			
ListSubscriptions	Concede permiso para enumerar las suscripciones para el plan de mantenimiento extendido (EMP) de FreeRTOS	Enumeración			
UpdateEmailRecipients	Concede permiso para actualizar la lista de las direcciones de correo electrónico de suscripción para el plan de mantenimiento extendido (EMP) de FreeRTOS	Escritura			
UpdateSoftwareConfiguration	Concede permiso para actualizar la configuración de software	Escritura	configuration*		
VerifyEmail	Concede permiso para verificar el correo electrónico para el plan de mantenimiento extendido (EMP) de FreeRTOS	Escritura			

Tipos de recursos definidos por Amazon FreeRTOS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
configuration	`arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}`	aws:ResourceTag/${TagKey}
subscription	`arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon FreeRTOS

Amazon FreeRTOS define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave de etiqueta presente en la solicitud que el usuario realiza a Amazon FreeRTOS	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por el componente de clave de etiqueta asociado a un recurso de Amazon FreeRTOS	Cadena
aws:TagKeys	Filtra el acceso en función de la lista de todos los nombres de clave de etiqueta asociados con el recurso en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon FSx

Amazon FSx (prefijo de servicio:`fsx`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon FSx
- Tipos de recursos definidos por Amazon FSx
- Claves de estado de Amazon FSx

Acciones definidas por Amazon FSx

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateFileGateway [solo permiso]	Otorga permiso para asociar una instancia de File Gateway a un sistema de archivos de Amazon FSx para Windows File Server	Escritura	file-system*		
AssociateFileSystemAliases	Otorga permiso para asociar alias de DNS a un sistema de archivos de Amazon FSx para Windows File Server	Escritura	file-system*		
BypassSnaplockEnterpriseRetention [solo permiso]	Otorga permiso para permitir la eliminación de un FSx volumen de ONTAP SnapLock Enterprise que contenga archivos WORM (escribir una vez, leer muchos) con períodos de retención activos	Administración de permisos	volume*		
CancelDataRepositoryTask	Concede permiso para cancelar una tarea de repositorio de datos.	Write	task*		
CopyBackup	Concede permiso para copiar una copia de seguridad	Escritura	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CopySnapshotAndUpdateVolume	Concede permiso para actualizar un volumen existente mediante una instantánea de otro sistema de archivos Amazon FSx for OpenZFS	Escritura	snapshot*		
			volume*		
CreateAndAttachS3AccessPoint	Otorga permiso para crear y adjuntar un punto de acceso S3 a un sistema de archivos FSx	Escritura	volume		s3:CreateAccessPoint s3:GetAccessPoint s3:PutAccessPointPolicy
CreateBackup	Concede permiso para crear una nueva copia de seguridad de un sistema de FSx archivos de Amazon o un FSx volumen de Amazon	Escritura	backup*		fsx:TagResource
			file-system		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataRepositoryAssociation	Concede permiso para crear una nueva asociación de repositorios de datos para un sistema de archivos Amazon FSx for Lustre	Escritura	association*		fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	Otorga permiso para crear una nueva tarea de repositorio de datos para un sistema de archivos Amazon FSx for Lustre	Escritura	file-system*		fsx:TagResource
			task*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFileCache	Concede permiso para crear una nueva caché de un archivo Amazon vacía	Escritura	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	Otorga permiso para crear un nuevo sistema de FSx archivos de Amazon vacío	Escritura	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	Concede permiso para crear un nuevo sistema de FSx archivos de Amazon a partir de una copia de seguridad existente	Escritura	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Concede permiso para crear una nueva instantánea en un volumen.	Escritura	snapshot*		fsx:TagResource
			volume*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageVirtualMachine	Concede permiso para crear una nueva máquina virtual de almacenamiento en un sistema de archivos Amazon FSx for Ontap	Escritura	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	Concede permiso para crear un nuevo volumen	Escritura	volume*		fsx:TagResource
			snapshot		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	Concede permiso para crear un nuevo volumen de copia de seguridad	Escritura	backup*		fsx:TagResource
			storage-virtual-machine*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBackup	Concede permiso para eliminar una copia de seguridad y su contenido. Después de la eliminación, la copia de seguridad ya no existe y sus datos ya no se encuentran disponibles.	Escritura	backup*		
DeleteDataRepositoryAssociation	Concede permiso para eliminar una asociación de repositorio de datos.	Escritura	association*		
DeleteFileCache	Concede permiso para eliminar la caché de un archivo y su contenido	Escritura	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFileSystem	Concede permiso para eliminar un sistema de archivos, su contenido y cualquier copia de seguridad automática existente de dicho sistema de archivos.	Escritura	file-system*		fsx:CreateBackup fsx:TagResource
			backup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [solo permiso]	Necesario para gestionar el uso compartido de FSx volúmenes entre cuentas mediante AWS Resource Access Manager (RAM). PutResourcePolicy y también GetResourcePolicy son necesarios	Administración de permisos	volume*		
DeleteSnapshot	Concede permiso para eliminar una instantánea en un volumen.	Escritura	snapshot*		
DeleteStorageVirtualMachine	Concede permiso para eliminar una máquina virtual de almacenamiento y su contenido.	Escritura	storage-virtual-machine*		
DeleteVolume	Concede permiso para eliminar un volumen, su contenido y cualquier copia de seguridad automática existente del volumen.	Escritura	volume*		fsx:TagResource
			backup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [solo permiso]	Otorga permiso para describir las instancias de File Gateway asociadas a un sistema de archivos de Amazon FSx para Windows File Server	Lectura	file-system*		
DescribeBackups	Otorga permiso para devolver las descripciones de todas las copias de seguridad Región de AWS de su propiedad Cuenta de AWS en el punto final al que llama	Lectura			
DescribeDataRepositoryAssociations	Otorga permiso para devolver las descripciones de todas las asociaciones de repositorios de datos Región de AWS de su propiedad Cuenta de AWS en el punto final al que llama	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDataRepositoryTasks	Otorga permiso para devolver las descripciones de todas las tareas del repositorio de datos Región de AWS de su propiedad Cuenta de AWS en el punto final al que llama	Lectura			
DescribeFileCaches	Otorga permiso para devolver las descripciones de todas las cachés de archivos Región de AWS de su propiedad Cuenta de AWS en el punto final al que llama	Lectura			
DescribeFileSystemAliases	Otorga permiso para devolver la descripción de todos los alias DNS propiedad de su sistema de archivos de Amazon FSx para Windows File Server	Lectura	file-system*		
DescribeFileSystems	Otorga permiso para devolver las descripciones de todos los sistemas de archivos Región de AWS de tu propiedad Cuenta de AWS en el punto final al que llamas	Lectura			
DescribeS3AccessPointAttachments	Otorga permiso para devolver las descripciones de los archivos adjuntos a los puntos de acceso S3	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSharedVpcConfiguration	Otorga permiso para devolver las descripciones de si se permite o no actualizar la tabla de FSx rutas desde las cuentas de los participantes en su cuenta	Lectura			
DescribeSnapshots	Otorga permiso para devolver las descripciones de todas las instantáneas que poseas Cuenta de AWS en el punto Región de AWS de conexión al que llamas	Lectura			
DescribeStorageVirtualMachines	Otorga permiso para devolver las descripciones de todas las máquinas virtuales de almacenamiento Región de AWS de su propiedad Cuenta de AWS en el punto final al que llama	Lectura			
DescribeVolumes	Otorga permiso para devolver las descripciones de todos los volúmenes Región de AWS de su propiedad Cuenta de AWS en el punto final al que llama	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetachAndDeleteS3AccessPoint	Otorga permiso para separar un punto de acceso S3 de un sistema de FSx archivos de Amazon y eliminar el punto de acceso S3	Escritura	volume		s3:DeleteAccessPoint
DisassociateFileGateway [solo permiso]	Concede permiso para desasociar una instancia de File Gateway de un sistema de archivos de Amazon FSx para Windows File Server	Escritura	file-system*		
DisassociateFileSystemAliases	Concede permiso para desasociar los alias del sistema de archivos con un sistema de archivos de Amazon FSx para Windows File Server	Escritura	file-system*		
GetResourcePolicy [solo permiso]	Necesario para gestionar el uso compartido de FSx volúmenes entre cuentas mediante AWS Resource Access Manager (RAM). PutResourcePolicy y también DeleteResourcePolicy son necesarios	Administración de permisos	volume*		
ListTagsForResource	Otorga permiso para enumerar etiquetas para un FSx recurso de Amazon	Lectura	association		
			backup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
ManageBackupPrincipalAssociations [solo permiso]	Otorga permiso para administrar las principales asociaciones de backup a través de AWS Backup	Administración de permisos	backup*		
PutResourcePolicy [solo permiso]	Necesario para gestionar el uso compartido de FSx volúmenes entre cuentas mediante AWS Resource Access Manager (RAM). DeleteResourcePolicy y también GetResourcePolicy son necesarios	Administración de permisos	volume*		
ReleaseFileSystemNfsV3Locks	Concede permiso para liberar bloqueos del sistema de archivos NFS V3	Escritura	file-system*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreVolumeFromSnapshot	Concede permiso para restaurar el estado del volumen a partir de una instantánea.	Escritura	snapshot*		
			volume*		
StartMisconfiguredStateRecovery	Concede permiso para iniciar la recuperación de estados mal configurados	Escritura	file-system*		
TagResource	Otorga permiso para etiquetar un FSx recurso de Amazon	Etiquetado	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una etiqueta de un FSx recurso de Amazon	Etiquetado	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys	
UpdateDataRepositoryAssociation	Concede permiso para actualizar la configuración de asociación del repositorios de datos.	Escritura	association*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFileCache	Concede permiso para actualizar la configuración de la caché de archivos	Escritura	file-cache*		
UpdateFileSystem	Concede permiso para actualizar la configuración del sistema de archivos.	Escritura	file-system*		
UpdateSharedVpcConfiguration	Otorga permiso para habilitar o deshabilitar las actualizaciones de la tabla de FSx rutas desde las cuentas de los participantes de su cuenta	Escritura			
UpdateSnapshot	Concede permiso para actualizar la configuración de la instancia.	Escritura	snapshot*		
UpdateStorageVirtualMachine	Concede permiso para actualizar la configuración de máquinas virtuales de almacenamiento	Escritura	storage-virtual-machine*		
UpdateVolume	Concede permiso para actualizar la configuración del volumen	Escritura	volume*		
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Tipos de recursos definidos por Amazon FSx

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> Amazon FSx for Windows File Server, Lustre y Ontap comparten algunos de los mismos tipos de recursos, con el mismo formato de ARN para cada uno.

Tipos de recurso	ARN	Claves de condición
file-system	`arn:${Partition}:fsx:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
file-cache	`arn:${Partition}:fsx:${Region}:${Account}:file-cache/${FileCacheId}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}`	aws:ResourceTag/${TagKey}
storage-virtual-machine	`arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey}
association	`arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
volume	`arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon FSx

Amazon FSx define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
fsx:IsBackupCopyDestination	Filtra el acceso en función de si la copia de seguridad es una copia de seguridad de destino para una CopyBackup operación	Bool

Claves de condición	Descripción	Tipo
fsx:IsBackupCopySource	Filtra el acceso en función de si la copia de seguridad es una copia de seguridad de origen para una CopyBackup operación	Bool
fsx:NfsDataRepositoryAuthenticationEnabled	Filtra el acceso por los repositorios de datos de NFS que admiten la autenticación	Bool
fsx:NfsDataRepositoryEncryptionInTransitEnabled	Filtra el acceso mediante los repositorios de datos NFS compatibles encryption-in-transit	Bool
fsx:ParentVolumeId	Filtra el acceso mediante el volumen primario contenedor para operaciones de volumen cambiantes	Cadena
fsx:StorageVirtualMachineId	Filtra el acceso de la máquina virtual de almacenamiento que contiene para un volumen para mutar operaciones de volumen	Cadena

Claves de condición, recursos y acciones para Amazon GameLift Servers

Amazon GameLift Servers (prefijo de servicio:`gamelift`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon GameLift Servers
- Tipos de recursos definidos por Amazon GameLift Servers
- Claves de condición para Amazon GameLift Servers

Acciones definidas por Amazon GameLift Servers

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptMatch	Otorga permiso para registrar a los jugadores que aceptan o rechazan un partido propuesto FlexMatch	Escritura			
ClaimGameServer	Otorga permiso para localizar y reservar un servidor de juego a fin de alojar una sesión de juego nueva	Write	gameServerGroup*		
CreateAlias	Otorga permiso para definir un alias nuevo para una flota	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateBuild	Otorga permiso para crear una compilación de juego nueva con archivos almacenados en un bucket de Amazon S3	Escritura		aws:RequestTag/${TagKey}	gamelift:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	iam:PassRole s3:GetObject
CreateContainerFleet	Otorga permiso para crear una nueva flota de contenedores con recursos informáticos para ejecutar tus servidores de juegos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateContainerGroupDefinition	Otorga permiso para crear una nueva definición de grupo de contenedores a partir de imágenes almacenadas en un repositorio de Amazon ECR	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer gamelift:TagResource
CreateFleet	Otorga permiso para crear una flota de recursos informáticos nueva a fin de ejecutar los servidores de juegos	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFleetLocations	Otorga permiso para especificar ubicaciones adicionales para una flota	Write	containerFleet		ec2:DescribeAvailabilityZones ec2:DescribeRegions
			fleet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGameServerGroup	Otorga permiso para crear un grupo de servidores de juegos nuevo, configurar un grupo de Auto Scaling correspondiente y lanzar instancias a fin de alojar servidores de juegos	Write		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule events:PutTargets

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					gamelift:TagResource iam:PassRole
CreateGameSession	Otorga permiso para iniciar una sesión de juego nueva en una flota especificada	Write			
CreateGameSessionQueue	Otorga permiso para configurar una cola nueva a fin de procesar solicitudes de ubicación de sesión de juego	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	Otorga permiso para definir una nueva ubicación para una flota	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingConfiguration	Otorga permiso para crear un nuevo emparejador FlexMatch	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMatchmakingRuleSet	Otorga permiso para crear un nuevo conjunto de reglas de emparejamiento para FlexMatch	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	Otorga permiso para reservar un espacio de sesión de juego disponible para un jugador	Write			
CreatePlayerSessions	Otorga permiso para reservar espacios de sesión de juego disponibles para varios jugadores	Write			
CreateScript	Otorga permiso para crear una secuencia de comandos de Realtime Servers nueva	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVpcPeeringAuthorization	Otorga permiso GameLift para crear o eliminar una conexión de emparejamiento entre una VPC de GameLift flota y una VPC de otra Cuenta de AWS	Escritura			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	Otorga permiso para establecer una conexión de emparejamiento entre la VPC de su GameLift flota y una VPC de otra cuenta	Escritura			
DeleteAlias	Otorga permiso para eliminar un alias	Write	alias*		
DeleteBuild	Otorga permiso para eliminar una compilación de juego	Escritura	build*		
DeleteContainerFleet	Otorga permiso para eliminar una flota de contenedores	Escritura	containerFleet*		
DeleteContainerGroupDefinition	Otorga permiso para eliminar una definición de grupo de contenedores	Escritura	containerGroupDefinition*		
DeleteFleet	Otorga permiso para eliminar una flota vacía	Write	fleet*		
DeleteFleetLocations	Otorga permiso para eliminar ubicaciones de una flota	Write	containerFleet		
			fleet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteGameServerGroup	Otorga permiso para eliminar permanentemente un grupo de servidores de juegos y finalizar la actividad de FleetIQ para el grupo de Auto Scaling correspondiente	Write	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	Otorga permiso para eliminar una cola de sesión de juego existente	Escritura	gameSessionQueue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLocation	Otorga permiso para eliminar una ubicación	Escritura	location*		
DeleteMatchmakingConfiguration	Otorga permiso para eliminar un FlexMatch emparejador existente	Escritura	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	Otorga permiso para eliminar un conjunto de reglas de FlexMatch emparejamiento existente	Escritura	matchmakingRuleSet*		
DeleteScalingPolicy	Otorga permiso para eliminar un conjunto de reglas de escalado automático	Write	containerFleet		
			fleet		
DeleteScript	Otorga permiso para eliminar una secuencia de comandos de servidores en tiempo real	Write	script*		
DeleteVpcPeeringAuthorization	Otorga permiso para cancelar una autorización de interconexión de VPC	Escritura			
DeleteVpcPeeringConnection	Otorga permiso para eliminar una conexión de emparejamiento entre VPCs	Escritura			
DeregisterCompute	Otorga permiso para anular el registro de un proceso de una flota	Escritura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterGameServer	Otorga permiso para eliminar un servidor de juegos de un grupo de servidores de juegos	Write	gameServerGroup*		
DescribeAlias	Otorga permiso para recuperar propiedades de un alias	Read	alias*		
DescribeBuild	Otorga permiso para recuperar propiedades de una compilación de juego	Lectura	build*		
DescribeCompute	Otorga permiso para recuperar información para un cómputo de una flota	Lectura	containerFleet		
			fleet		
DescribeContainerFleet	Otorga permiso para recuperar las propiedades de una flota de contenedores existente	Lectura	containerFleet*		
DescribeContainerGroupDefinition	Otorga permiso para recuperar las propiedades de una definición de grupo de contenedores existente	Lectura	containerGroupDefinition*		
DescribeEC2InstanceLimits	Otorga permiso para recuperar el uso máximo permitido y actual de los tipos de EC2 instancias	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFleetAttributes	Otorga permiso para recuperar propiedades generales, incluido el estado, para flotas	Lectura			
DescribeFleetCapacity	Otorga permiso para recuperar la configuración de capacidad actual de las flotas gestionadas	Lectura			
DescribeFleetDeployment	Otorga permiso para recuperar las propiedades de un despliegue de flota existente	Lectura	containerFleet*		
DescribeFleetEvents	Otorga permiso para recuperar entradas del registro de eventos de una flota	Read	containerFleet		
			fleet		
DescribeFleetLocationAttributes	Otorga permiso para recuperar propiedades generales, incluidos los estados, de las ubicaciones de una flota	Read	containerFleet		
			fleet		
DescribeFleetLocationCapacity	Otorga permiso para recuperar la configuración de capacidad actual para la ubicación de una flota	Read	containerFleet		
			fleet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFleetLocationUtilization	Otorga permiso para recuperar estadísticas de utilización para la ubicación de la flota	Read	fleet*		
DescribeFleetPortSettings	Otorga permiso para recuperar los permisos de conexión entrante para una flota	Read	fleet*		
DescribeFleetUtilization	Otorga permiso para recuperar estadísticas de utilización de flotas	Read			
DescribeGameServer	Otorga permiso para recuperar propiedades de un servidor de juegos	Read	gameServerGroup*		
DescribeGameServerGroup	Otorga permiso para recuperar propiedades de un grupo de servidores de juegos	Lectura	gameServerGroup*		
DescribeGameServerInstances	Otorga permiso para recuperar el estado de las EC2 instancias de un grupo de servidores de juegos	Lectura	gameServerGroup*		
DescribeGameSessionDetails	Otorga permiso para recuperar propiedades de sesiones de juego en una flota, incluida la política de protección	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeGameSessionPlacement	Otorga permiso para recuperar detalles de una solicitud de ubicación de sesión de juego	Read			
DescribeGameSessionQueues	Otorga permiso para recuperar propiedades de colas de sesiones de juego	Read			
DescribeGameSessions	Otorga permiso para recuperar propiedades de sesiones de juego en una flota	Lectura			
DescribeInstances	Otorga permiso para recuperar información sobre las instancias de una flota gestionada	Lectura	containerFleet		
			fleet		
DescribeMatchmaking	Otorga permiso para recuperar detalles de tickets de emparejamiento	Lectura			
DescribeMatchmakingConfigurations	Otorga permiso para recuperar propiedades a los FlexMatch emparejadores	Lectura			
DescribeMatchmakingRuleSets	Otorga permiso para recuperar propiedades para conjuntos de FlexMatch reglas de emparejamiento	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePlayerSessions	Otorga permiso para recuperar propiedades de sesiones de jugador en una sesión de juego	Read			
DescribeRuntimeConfiguration	Otorga permiso para recuperar la configuración actual de tiempo de ejecución para una flota	Read	fleet*		
DescribeScalingPolicies	Otorga permiso para recuperar todas las políticas de escalado que se aplican a una flota	Read	containerFleet		
			fleet		
DescribeScript	Otorga permiso para recuperar propiedades de una secuencia de comandos de Realtime Servers	Read	script*		
DescribeVpcPeeringAuthorizations	Otorga permiso para recuperar autorizaciones de interconexión de VPC válidas	Read			
DescribeVpcPeeringConnections	Otorga permiso para recuperar detalles en conexiones de interconexión de VPC activas o pendientes	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetComputeAccess	Otorga permiso para recuperar credenciales para acceder de forma remota a un ordenador de una flota gestionada	Lectura	containerFleet		
			fleet		
GetComputeAuthToken	Otorga permiso para recuperar un token de autenticación que permite a los procesos de un ordenador enviar solicitudes al GameLift servicio de Amazon	Lectura	containerFleet		
			fleet		
GetGameSessionLogUrl	Otorga permiso para recuperar la ubicación de los registros almacenados para una sesión de juego	Read			
GetInstanceAccess	Otorga permiso para solicitar acceso remoto a una instancia de flota especificada	Read	fleet*		
ListAliases	Otorga permiso para recuperar todos los alias definidos en la región actual	List			
ListBuilds	Otorga permiso para recuperar toda la compilación del juego de la región actual	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCompute	Otorga permiso para recuperar todos los recursos de computación de la región actual	Enumeración	containerFleet		
			fleet		
ListContainerFleets	Otorga permiso para recuperar las propiedades de todas las flotas de contenedores existentes en la región actual	Enumeración			
ListContainerGroupDefinitionVersions	Otorga permiso para recuperar las propiedades de todas las versiones de una definición de grupo de contenedores existente	Enumeración	containerGroupDefinition*		
ListContainerGroupDefinitions	Otorga permiso para recuperar las propiedades de todas las definiciones de grupos de contenedores existentes en la región actual	Enumeración			
ListFleetDeployments	Otorga permiso para recuperar las propiedades de todos los despliegues de flota existentes en la región actual	Enumeración			
ListFleets	Otorga permiso para recuperar una lista de la flota IDs de todas las flotas de la región actual	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGameServerGroups	Otorga permiso para recuperar todos los grupos de servidores de juegos definidos en la región actual	List			
ListGameServers	Otorga permiso para recuperar todos los servidores de juegos que se ejecutan actualmente en un grupo de servidores de juegos	Enumeración	gameServerGroup*		
ListLocations	Otorga permiso para recuperar todas las ubicaciones de esta cuenta	Enumeración			
ListScripts	Otorga permiso para recuperar propiedades de todos los scripts de Realtime Servers de la región actual	Enumeración			
ListTagsForResource	Otorga permiso para recuperar las etiquetas de los recursos GameLift	Lectura	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
PutScalingPolicy	Otorga permiso para crear o actualizar una política de escalado automático de flotas	Escritura	containerFleet		
			fleet		
RegisterCompute	Otorga permiso para registrar un proceso en una flota	Escritura	fleet*		
RegisterGameServer	Otorga permiso para notificar a GameLift FleetiQ cuando un nuevo servidor de juegos esté listo para albergar el juego	Escritura	gameServerGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RequestUploadCredentials	Otorga permiso para recuperar credenciales de carga nuevas a fin de utilizarlas al cargar una compilación de juego nueva	Read	build*		
ResolveAlias	Otorga permiso para recuperar el ID de flota asociado a un alias	Read	alias*		
ResumeGameServerGroup	Otorga permiso para restablecer la actividad suspendida de FleetIQ para un grupo de servidores de juegos	Write	gameServerGroup*		
SearchGameSessions	Otorga permiso para recuperar sesiones de juego que coinciden con un conjunto de criterios de búsqueda	Lectura			
StartFleetActions	Otorga permiso para reanudar la actividad de autoscalamiento en una flota después de suspenderla con StopFleetActions ()	Escritura	containerFleet		
			fleet		
StartGameSessionPlacement	Otorga permiso para enviar una solicitud de ubicación de sesión de juego a una cola de sesión de juego	Escritura	gameSessionQueue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartMatchBackfill	Otorga permiso para solicitar el FlexMatch emparejamiento para cubrir los espacios disponibles para los jugadores en una sesión de juego existente	Escritura			
StartMatchmaking	Otorga permiso para solicitar el FlexMatch emparejamiento de uno o un grupo de jugadores e iniciar la sesión de juego	Escritura			
StopFleetActions	Otorga permiso para suspender la actividad de escalado automático en una flota	Write	containerFleet		
			fleet		
StopGameSessionPlacement	Otorga permiso para cancelar una solicitud de ubicación de sesión de juego que está en curso	Write			
StopMatchmaking	Otorga permiso para cancelar una solicitud de emparejamiento o relleno de coincidencias que está en curso	Write			
SuspendGameServerGroup	Otorga permiso para detener temporalmente la actividad de FleetIQ para un grupo de servidores de juegos	Escritura	gameServerGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar los recursos GameLift	Etiquetado	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateGameSession	Otorga permiso para cerrar una sesión de juego existente	Escritura			
UntagResource	Otorga permiso para eliminar la etiqueta de GameLift los recursos	Etiquetado	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:TagKeys	
UpdateAlias	Otorga permiso para actualizar las propiedades de un alias existente	Write	alias*		
UpdateBuild	Otorga permiso para actualizar los metadatos de una compilación existente	Escritura	build*		
UpdateContainerFleet	Otorga permiso para actualizar una flota de contenedores existente	Escritura	containerFleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateContainerGroupDefinition	Otorga permiso para actualizar las propiedades de una definición de grupo de contenedores existente	Escritura	containerGroupDefinition*		ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer
UpdateFleetAttributes	Otorga permiso para actualizar las propiedades generales de una flota existente	Escritura	fleet*		
UpdateFleetCapacity	Otorga permiso para ajustar la configuración de capacidad de una flota gestionada	Escritura	containerFleet		
			fleet		
UpdateFleetPortSettings	Otorga permiso para ajustar la configuración de puerto de una flota	Write	fleet*		
UpdateGameServer	Otorga permiso para cambiar las propiedades del servidor de juegos, el estado de mantenimiento o estado de utilización	Write	gameServerGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGameServerGroup	Otorga permiso para actualizar las propiedades del grupo de servidores de juegos, incluidos los tipos de instancia permitidos	Write	gameServerGroup*		iam:PassRole
UpdateGameSession	Otorga permiso para actualizar las propiedades de una sesión de juego existente	Write			
UpdateGameSessionQueue	Otorga permiso para actualizar las propiedades de una cola de sesión de juego existente	Escritura	gameSessionQueue*		
UpdateMatchmakingConfiguration	Otorga permiso para actualizar las propiedades de una configuración de FlexMatch emparejamiento existente	Escritura	matchmakingConfiguration*		
UpdateRuntimeConfiguration	Otorga permiso para actualizar cómo se configuran los procesos de servidor en instancias de una flota existente	Write	fleet*		
UpdateScript	Otorga permiso para actualizar los metadatos y el contenido de una secuencia de comandos de Realtime Servers existente	Escritura	script*		iam:PassRole s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ValidateMatchmakingRuleSet	Otorga permiso para validar la sintaxis de un conjunto de reglas de FlexMatch emparejamiento	Lectura			

Tipos de recursos definidos por Amazon GameLift Servers

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
alias	`arn:${Partition}:gamelift:${Region}::alias/${AliasId}`	aws:ResourceTag/${TagKey}
build	`arn:${Partition}:gamelift:${Region}:${Account}:build/${BuildId}`	aws:ResourceTag/${TagKey}
containerGroupDefinition	`arn:${Partition}:gamelift:${Region}:${Account}:containergroupdefinition/${Name}`	aws:ResourceTag/${TagKey}
containerFleet	`arn:${Partition}:gamelift:${Region}:${Account}:containerfleet/${FleetId}`	aws:ResourceTag/${TagKey}
fleet	`arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
gameServerGroup	arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}	aws:ResourceTag/${TagKey}
gameSessionQueue	arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}	aws:ResourceTag/${TagKey}
matchmakingConfiguration	arn:${Partition}:gamelift:${Region}:${Account}:matchmakingconfiguration/${MatchmakingConfigurationName}	aws:ResourceTag/${TagKey}
matchmakingRuleSet	arn:${Partition}:gamelift:${Region}:${Account}:matchmakingruleset/${MatchmakingRuleSetName}	aws:ResourceTag/${TagKey}
script	arn:${Partition}:gamelift:${Region}:${Account}:script/${ScriptId}	aws:ResourceTag/${TagKey}

Claves de condición para Amazon GameLift Servers

Amazon GameLift Servers define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon GameLift Streams

Amazon GameLift Streams (prefijo de servicio:`gameliftstreams`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon GameLift Streams
- Tipos de recursos definidos por Amazon GameLift Streams
- Claves de condición de Amazon GameLift Streams

Acciones definidas por Amazon GameLift Streams

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddStreamGroupLocations	Otorga permiso para adjuntar una ubicación StreamGroup remota	Escritura	streamgroup*		ec2:DescribeRegions
AssociateApplications	Otorga permiso para asociar aplicaciones a un StreamGroup	Escritura	application*		
			streamgroup*		
CreateApplication	Otorga permiso para crear una aplicación.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource s3:GetObject s3:ListBucket
CreateStreamGroup	Otorga permiso para crear un StreamGroup	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource
CreateStreamSessionConnection	Otorga permiso para crear una conexión de sesión de streaming	Escritura	streamgroup*		
DeleteApplication	Concede permiso para eliminar una aplicación.	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteStreamGroup	Otorga permiso para eliminar un StreamGroup	Escritura	streamgroup*		
DisassociateApplications	Otorga permiso para desvincular las aplicaciones de un StreamGroup	Escritura	application*		
			streamgroup*		
ExportStreamSessionFiles	Otorga permiso para exportar los archivos de sesión de streaming que genere su aplicación	Escritura	streamgroup*		s3:PutObject
GetApplication	Concede el permiso para obtener una aplicación	Lectura	application*		
GetStreamGroup	Otorga un `permiso` para obtener un StreamGroup	Lectura	streamgroup*		
GetStreamSession	Otorga permiso para obtener una sesión de streaming	Lectura	streamgroup*		
ListApplications	Concede permiso para enumerar las aplicaciones.	Enumeración			
ListStreamGroups	Otorga permiso para publicar StreamGroups	Enumeración			
ListStreamSessions	Otorga permiso para enumerar las sesiones de streaming	Lectura	streamgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStreamSessionsByAccount	Otorga permiso para enumerar las sesiones de transmisión	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	application		
			streamgroup		
RemoveStreamGroupLocations	Otorga permiso para separar una ubicación StreamGroup remota	Escritura	streamgroup*		
StartStreamSession	Otorga permiso para crear una sesión de transmisión	Escritura	streamgroup*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	application		
			streamgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateStreamSession	Otorga permiso para terminar una sesión de transmisión	Escritura	streamgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	application		
			streamgroup		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	application*		
UpdateStreamGroup	Otorga permiso para actualizar un StreamGroup	Escritura	streamgroup*		

Tipos de recursos definidos por Amazon GameLift Streams

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:gameliftstreams:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
stream group	`arn:${Partition}:gameliftstreams:${Region}:${Account}:streamgroup/${StreamGroupId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon GameLift Streams

Amazon GameLift Streams define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Global Accelerator

AWS Global Accelerator (prefijo de servicio:`globalaccelerator`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Global Accelerator
- Tipos de recursos definidos por AWS Global Accelerator
- Claves de condición para AWS Global Accelerator

Acciones definidas por AWS Global Accelerator

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddCustomRoutingEndpoints	Otorga permiso para agregar un punto de enlace de subred de Virtual Private Cloud (VPC) a un grupo de puntos de conexión del acelerador de direccionamiento personalizado.	Escritura	endpointgroup*		
AddEndpoints	Concede permiso para agregar un punto de conexión a un grupo de puntos de conexión de un acelerador estándar	Escritura	endpointgroup*		globalaccelerator:UpdateEndpointGroup
AdvertiseByoipCidr	Otorga permiso para anunciar un rango de IPv4 direccion	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	es aprovisionado para su uso con el acelerador mediante el uso de direcciones IP propias (BYOIP)				
AllowCustomRoutingTraffic	Otorga permiso para permitir el enrutamiento personalizado del tráfico de usuario a un puerto IP: PORT de destino privado en una subred de VPC específica.	Escritura	endpointgroup*		
CreateAccelerator	Otorga permiso para crear un acelerador estándar	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAttachment	Otorga permiso para crear un CrossAccountAttachment	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingAccelerator	Otorga permiso para crear un acelerador de direccionamiento personalizado.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCustomRoutingEndpointGroup	Otorga permiso para crear un grupo de puntos de conexión del agente de escucha especificado de un acelerador de enrutamiento personalizado.	Escritura	listener*		
CreateCustomRoutingListener	Otorga permiso para crear un agente de escucha para procesar conexiones entrantes de clientes a un acelerador de enrutamiento personalizado.	Escritura	accelerator*		
CreateEndpointGroup	Otorga permiso para agregar un grupo de puntos de conexión a un agente de escucha de un acelerador estándar.	Escritura	listener*		
CreateListener	Otorga permiso para agregar un agente de escucha a un acelerador estándar	Escritura	accelerator*		
DeleteAccelerator	Otorga permiso para eliminar un acelerador estándar	Escritura	accelerator*		
DeleteCrossAccountAttachment	Otorga permiso para eliminar un CrossAccountAttachment	Escritura	attachment*		
DeleteCustomRoutingAccelerator	Otorga permiso para eliminar un acelerador de enrutamiento personalizado	Escritura	accelerator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCustomRoutingEndpointGroup	Otorga permiso para eliminar un grupo de puntos de conexión de un agente de escucha de un acelerador de enrutamiento personalizado.	Escritura	endpointgroup*		
DeleteCustomRoutingListener	Otorga permiso para eliminar un agente de escucha de un acelerador de enrutamiento personalizado.	Escritura	listener*		
DeleteEndpointGroup	Otorga permiso para eliminar un grupo de puntos de conexión asociado a un agente de escucha de un acelerador estándar.	Escritura	endpointgroup*		
DeleteListener	Otorga permiso para eliminar un agente de escucha de un acelerador estándar	Escritura	listener*		
DenyCustomRoutingTraffic	Otorga permiso para no permitir el enrutamiento personalizado del tráfico de usuario a un puerto IP:PORT de destino privado en una subred de una VPC específica	Escritura	endpointgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeprovisionByoipCidr	Otorga permiso para liberar el rango de direcciones especificado que aprovisionó para su uso con su acelerador a través de direcciones Bring Your Own IP (BYOIP)	Escritura			
DescribeAccelerator	Otorga permiso para describir un acelerador estándar	Lectura	accelerator*		
DescribeAcceleratorAttributes	Otorga permiso para describir los atributos de un acelerador estándar	Lectura	accelerator*		
DescribeCrossAccountAttachment	Otorga permisos para describir un CrossAccountAttachment	Lectura	attachment*		
DescribeCustomRoutingAccelerator	Otorga permiso para describir un acelerador de enrutamiento personalizado.	Lectura	accelerator*		
DescribeCustomRoutingAcceleratorAttributes	Otorga permiso para describir los atributos de un acelerador de enrutamiento personalizado	Lectura	accelerator*		
DescribeCustomRoutingEndpointGroup	Otorga permiso para describir un grupo de puntos de conexión de un acelerador de enrutamiento personalizado.	Lectura	endpointgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCustomRoutingListener	Otorga permiso para describir un agente de escucha de un acelerador de enrutamiento personalizado.	Lectura	listener*		
DescribeEndpointGroup	Otorga permiso para describir el grupo de puntos de conexión de un acelerador estándar.	Lectura	endpointgroup*		
DescribeListener	Otorga permiso para describir un agente de escucha de un acelerador estándar	Lectura	listener*		
ListAccelerators	Otorga permiso para mostrar una lista de todos los aceleradores estándar	Enumeración			
ListByoipCidrs	Otorga permiso para mostrar una lista de los CIDR BYOIP	Enumeración			
ListCrossAccountAttachments	Otorga permiso para enumerar todos CrossAccountAttachments	Enumeración			
ListCrossAccountResourceAccounts	Otorga permiso para incluir en la CrossAccountAttachments lista las cuentas en las que aparezca la persona que llama como principal	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCrossAccountResources	Otorga permiso para enumerar todos los CrossAccountAttachment recursos que puede utilizar la persona que llama	Enumeración			
ListCustomRoutingAccelerators	Otorga permiso para enumerar los aceleradores de enrutamiento personalizados de una Cuenta de AWS	Enumeración			
ListCustomRoutingEndpointGroups	Otorga permiso para mostrar una lista de los grupos de puntos de conexión asociados a un agente de escucha de un acelerador de enrutamiento personalizado.	Enumeración	listener*		
ListCustomRoutingListeners	Otorga permiso para mostrar una lista de los agentes de escucha de un acelerador de enrutamiento personalizado	Enumeración	accelerator*		
ListCustomRoutingPortMappings	Otorga permiso para mostrar una lista de los mapeos de puertos de un acelerador de enrutamiento personalizado.	Enumeración	accelerator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCustomRoutingPortMappingsByDestination	Otorga permiso para mostrar una lista de los mapeos de puertos de una dirección IP de punto de enlace específica (una dirección de destino) en una subred	Enumeración			
ListEndpointGroups	Otorga permiso para mostrar una lista de todos los grupos de puntos de conexión asociados a un agente de escucha de un acelerador estándar.	Enumeración	listener*		
ListListeners	Otorga permiso para mostrar una lista de todos los agentes de escucha asociados a un acelerador estándar	Enumeración	accelerator*		
ListTagsForResource	Otorga permiso para mostrar una lista de las etiquetas de un recurso globalaccelerator	Lectura	accelerator		
			attachment		
ProvisionByoipCidr	Con permiso para aprovisionar un rango de direcciones para su uso con su acelerador mediante Traiga sus propias direcciones IP (BYOIP)	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveCustomRoutingEndpoints	Otorga permiso para eliminar los puntos de enlace de subred de Virtual Private Cloud (VPC) de un grupo de puntos de conexión del acelerador de enrutamiento personalizado	Escritura	endpointgroup*		
RemoveEndpoints	Concede permiso para quitar un punto de conexión de un grupo de puntos de conexión de un acelerador estándar	Escritura	endpointgroup*		globalaccelerator:UpdateEndpointGroup
TagResource	Otorga permiso para agregar etiquetas a un recurso globalaccelerator	Etiquetado	accelerator		
			attachment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso globalaccelerator	Etiquetado	accelerator		
			attachment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateAccelerator	Otorga permiso para actualizar un acelerador estándar.	Escritura	accelerator*		
UpdateAcceleratorAttributes	Otorga permiso para actualizar los atributos de un acelerador estándar	Escritura	accelerator*		
UpdateCrossAccountAttachment	Otorga permiso para actualizar un CrossAccountAttachment	Escritura	attachment*		
UpdateCustomRoutingAccelerator	Otorga permiso para actualizar un acelerador de enrutamiento personalizado	Escritura	accelerator*		
UpdateCustomRoutingAcceleratorAttributes	Otorga permiso para actualizar los atributos de un acelerador de enrutamiento personalizado	Escritura	accelerator*		
UpdateCustomRoutingListener	Otorga permiso para actualizar un agente de escucha de un acelerador de enrutamiento personalizado	Escritura	listener*		
UpdateEndpointGroup	Otorga permiso para actualizar un grupo de puntos de conexión en un agente de escucha de un acelerador estándar.	Escritura	endpointgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateListener	Otorga permiso para actualizar un agente de escucha en un acelerador estándar.	Escritura	listener*		
WithdrawByoipCidr	Otorga permiso para dejar de anunciar una dirección BYOIP IPv4	Escritura			

Tipos de recursos definidos por AWS Global Accelerator

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
accelerator	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}`	aws:ResourceTag/${TagKey}
listener	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}`	aws:ResourceTag/${TagKey}
endpointgroup	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}/endpoint-group/${EndpointGroupId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
attachment	`arn:${Partition}:globalaccelerator::${Account}:attachment/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Global Accelerator

AWS Global Accelerator define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Glue

AWS Glue (prefijo de servicio:`glue`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Glue
- Tipos de recursos definidos por AWS Glue
- Claves de condición para AWS Glue

Acciones definidas por AWS Glue

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AuthorizeInboundIntegration [solo permiso]	Otorga permiso a Glue para validar continuamente que el ARN de destino puede recibir datos replicados desde el ARN de origen	Escritura	integration*		
BatchCreatePartition	Concede permiso para crear una o varias particiones	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteConnection	Concede permiso para eliminar una o varias conexiones	Write	connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			rootcatalog*		
BatchDeletePartition	Concede permiso para eliminar una o varias particiones	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTable	Concede permiso para eliminar una o varias tablas	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTableVersion	Concede permiso para eliminar una o varias versiones de una tabla	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetBlueprints	Concede permiso para recuperar uno o varios esquemas	Lectura	blueprint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetCrawlers	Concede permiso para recuperar uno o varios rastreadores	Lectura	crawler*		
BatchGetCustomEntityTypes	Concede permiso para recuperar uno o varios tipos de entidad personalizados	Lectura			
BatchGetDevEndpoints	Concede permiso para recuperar uno o varios puntos de enlace de desarrollo	Read	devendpoint*		
BatchGetJobs	Concede permiso para recuperar uno o varios trabajos	Read	job*		
BatchGetPartition	Concede permiso para recuperar una o varias particiones	Lectura	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetStageFiles	Concede permiso para obtener por lotes archivos de etapa para SparkUI	Administración de permisos			
BatchGetTableOptimizer	Concede permiso para devolver la configuración para los optimizadores de tablas especificados	Lectura	database*		glue:GetTable
			rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			table*		
BatchGetTriggers	Concede permiso para recuperar uno o varios disparadores	Read	trigger*		
BatchGetWorkflows	Concede permiso para recuperar uno o varios flujos de trabajo	Read	workflow*		
BatchStopJobRun	Concede permiso para detener una o más ejecuciones de trabajo de un trabajo	Escritura	job*		
BatchUpdatePartition	Concede permiso para actualizar una o varias particiones	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
CancelDataQualityRuleRecommendationRun	Otorga permiso para detener la ejecución de una recomendación de regla de Calidad de datos en ejecución	Escritura	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	Otorga permiso para detener la ejecución de la evaluación de un conjunto de reglas de Calidad de datos	Escritura	dataQualityRuleset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelMLTaskRun	Concede permiso para detener una ML Task Run en ejecución	Escritura	mlTransform*		
CancelStatement	Concede permiso para cancelar una instrucción en una sesión interactiva	Escritura	session*		
CheckSchemaVersionValidity	Concede permiso para recuperar una comprobación de la validez de la versión de esquema	Lectura			
CreateBlueprint	Concede permiso para crear un esquema	Escritura	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	Otorga permiso para crear un catálogo	Escritura	catalog*		
			rootcatalog*		
CreateClassifier	Concede permiso para crear un clasificador	Escritura			
CreateColumnStatisticsTaskSettings	Otorga permiso para crear la configuración de una tarea de estadísticas de columnas	Escritura	database*		
			rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			table*		
CreateConnection	Concede permiso para crear una conexión	Write	rootcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrawler	Concede permiso para crear un rastreador	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomEntityType	Concede permiso para crear un tipo de entidad personalizada.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	Otorga permiso para crear un conjunto de reglas de Calidad de datos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatabase	Concede permiso para crear una base de datos	Write	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			rootcatalog*		
			catalog		
CreateDevEndpoint	Concede permiso para crear un punto de conexión de desarrollo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInboundIntegration [solo permiso]	Concede permiso al director de origen para crear una integración entrante para que los datos se repliquen del origen al destino	Escritura			
CreateIntegration	Otorga permiso para crear una integración	Escritura	catalog*		kms:CreateGrant kms:DescribeKey
			connection*		
			database*		
			integration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationResourceProperty	Otorga permiso para crear una propiedad de recurso de integración	Escritura	catalog*		
			connection*		
			database*		
CreateIntegrationTableProperties	Otorga permiso para crear las propiedades de la tabla de integración	Escritura	catalog*		
			connection*		
			database*		
CreateJob	Concede permiso para crear un trabajo.	Write	job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateMLTransform	Concede permiso para crear una transformación ML	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartition	Concede permiso para crear una partición	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
CreatePartitionIndex		Escritura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para crear un índice de partición especificado en una tabla existente		rootcatalog*		
			table*		
			catalog		
CreateRegistry	Concede permiso para crear un nuevo registro de esquemas	Write	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Concede permiso para crear un nuevo contenedor de esquemas	Write	registry*		
			schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	Concede permiso para crear un script.	Write			
CreateSecurityConfiguration	Concede permiso para crear una configuración de seguridad	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSession	Concede permiso para crear una sesión interactiva	Escritura	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateTable	Concede permiso para crear una tabla	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
CreateTableOptimizer	Concede permiso para crear un nuevo optimizador de tablas para una función específica. La compactación es el único tipo de optimizador compatible actualmente	Escritura	database*		glue:GetTable
			rootcatalog*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTrigger	Concede permiso para crear un disparador	Escritura	trigger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageProfile	Concede permiso para crear un perfil de uso	Escritura	usageProfile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserDefinedFunction	Concede permiso para crear una definición de función	Write	database*		
			rootcatalog*		
			catalog		
CreateWorkflow	Concede permiso para crear un flujo de trabajo	Escritura	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBlueprint	Concede permiso para eliminar un esquema	Escritura	blueprint*		
DeleteCatalog	Otorga permiso para eliminar un catálogo	Escritura	rootcatalog*		
			catalog		
DeleteClassifier	Concede permiso para eliminar un clasificador	Escritura			
DeleteColumnStatisticsForPartition	Concede permiso para eliminar las estadísticas de columnas de la partición de una columna	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsForTable	Concede permiso para eliminar las estadísticas de tabla de las columnas	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsTaskSettings	Otorga permiso para eliminar la configuración de una tarea de estadísticas de columnas	Escritura	database*		
			rootcatalog*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConnection	Concede permiso para eliminar una conexión.	Write	connection*		
			rootcatalog*		
DeleteCrawler	Concede permiso para eliminar un rastreador	Escritura	crawler*		
DeleteCustomEntityType	Concede permiso para eliminar un tipo de entidad personalizada	Escritura			
DeleteDataQualityRuleset	Otorga permiso para eliminar un conjunto de reglas de Calidad de datos	Escritura	dataQualityRuleset*		
DeleteDatabase	Concede permiso para eliminar una base de datos	Write	database*		
			rootcatalog*		
			table*		
			userdefinedfunction*		
			catalog		
DeleteDevEndpoint	Concede permiso para eliminar un punto de conexión de desarrollo	Escritura	devendpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIntegration	Otorga permiso para eliminar una integración	Escritura	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationTableProperties	Otorga permiso para eliminar las propiedades de la tabla de integración	Escritura	catalog*		
			connection*		
			database*		
DeleteJob	Concede permiso para eliminar un trabajo.	Write	job*		
DeleteMLTransform	Concede permiso para eliminar una transformación ML	Write	mlTransform*		
DeletePartition	Concede permiso para eliminar una partición	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
DeletePartitionIndex	Concede permiso para eliminar un índice de partición especificado en una tabla existente	Escritura	database*		
			rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			table*		
			catalog		
DeleteRegistry	Concede permiso para eliminar un registro de esquemas	Write	registry*		
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos	Permissions management	rootcatalog*		
DeleteSchema	Concede permiso para eliminar un contenedor de esquemas	Write	registry*		
			schema*		
DeleteSchemaVersions	Concede permiso para eliminar un rango de versiones de esquema	Write	registry*		
			schema*		
DeleteSecurityConfiguration	Concede permiso para eliminar una configuración de seguridad	Escritura			
DeleteSession	Concede permiso para eliminar una sesión interactiva tras detener la sesión si no se ha detenido ya	Escritura	session*		
DeleteTable	Concede permiso para eliminar una tabla	Escritura	database*		
			rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			table*		
			catalog		
DeleteTableOptimizer	Concede permiso para eliminar un optimizador y todos los metadatos asociados a una tabla. La optimización ya no se realizará en la tabla	Escritura	database*		glue:GetTable
			rootcatalog*		
			table*		
DeleteTableVersion	Concede permiso para eliminar una versión de una tabla	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTrigger	Concede permiso para eliminar un disparador	Escritura	trigger*		
DeleteUsageProfile	Concede permiso para eliminar un perfil de uso	Escritura	usageProfile*		
DeleteUserDefinedFunction	Concede permiso para eliminar una definición de función	Write	database*		
			rootcatalog*		
			userdefinedfunction*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			catalog		
DeleteWorkflow	Concede permiso para eliminar un flujo de trabajo	Escritura	workflow*		
DeregisterDataPreview	Otorga permiso para terminar la sesión de un bloc de notas de Glue Studio	Administración de permisos			
DescribeConnectionType	Concede permiso para describir el tipo de conexión en Glue Studio	Administración de permisos			
DescribeEntity	Concede permiso para describir la entidad en Glue Studio	Administración de permisos	connection*		
			rootcatalog*		
DescribeInboundIntegrations	Concede permiso para enumerar las integraciones entrantes	Enumeración			
DescribeIntegrations	Otorga permiso para describir las integraciones sin ETL	Enumeración	integration*		
				aws:ResourceTag/${TagKey}	
GetBlueprint	Concede permiso para recuperar un esquema	Lectura	blueprint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBlueprintRun	Concede permiso para recuperar una ejecución de esquema	Lectura	blueprint*		
GetBlueprintRuns	Concede permiso para recuperar todas las ejecuciones de un esquema	Lectura	blueprint*		
GetCatalog	Otorga permiso para recuperar un catálogo	Lectura	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetCatalogImportStatus	Concede permiso para recuperar el estado de importación del catálogo	Lectura	rootcatalog*		
GetCatalogs	Otorga permiso para recuperar todos los catálogos	Lectura	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetClassifier	Concede permiso para recuperar un clasificador	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetClassifiers	Concede permiso para crear una lista de todos los clasificadores	Lectura			
GetColumnStatisticsForPartition	Concede permiso para recuperar las estadísticas de partición de las columnas	Lectura	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsForTable	Concede permiso para recuperar las estadísticas de tabla de las columnas	Lectura	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsTaskRun	Concede permiso para recuperar información de ejecución de estadísticas de columnas para la tabla basada en identificadores de ejecución	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetColumnStatisticsTaskRuns	Concede permiso para recuperar la información de ejecución de las estadísticas de columnas de la tabla en función de los identificadores de ejecución	Lectura			
GetColumnStatisticsTaskSettings	Otorga permiso para recuperar la configuración de una tarea de estadísticas de columnas	Lectura			
GetCompletion	Otorga permiso para obtener una respuesta generada para una solicitud de finalización en Glue from AWS Q	Lectura	completion*		
GetConnection	Concede permiso para recuperar una conexión	Read	connection*		
			rootcatalog*		
GetConnections	Concede permiso para recuperar una lista de conexiones	Read	connection*		
			rootcatalog*		
GetCrawler	Concede permiso para recuperar un rastreador	Read	crawler*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCrawlerMetrics	Concede permiso para recuperar métricas sobre rastreadores	Read			
GetCrawlers	Otorga permiso para recuperar todos los rastreadores.	Lectura			
GetCustomEntityType	Concede permiso para leer un tipo de entidad personalizada.	Lectura			
GetDashboardUrl	Otorga permiso para generar una URL prefirmada para acceder a la interfaz de usuario de Spark Live	Lectura	session*		
GetDataCatalogEncryptionSettings	Concede permiso para recuperar la configuración de cifrado de catálogos	Lectura	rootcatalog*		
GetDataPreviewStatement	Concede permiso para obtener una instrucción de vista previa de datos	Administración de permisos			
GetDataQualityModel	Concede permiso para recuperar el estado de entrenamiento del modelo de predicción de una estadística	Lectura	dataQualityRuleset*		
			job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDataQualityModelResult	Concede permiso para recuperar las predicciones de una estadística a partir del modelo más reciente	Lectura	dataQualityRuleset*		
			job*		
GetDataQualityResult	Otorga permiso para recuperar un resultado de Calidad de datos	Lectura	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	Otorga permiso para recuperar una ejecución de recomendación de regla de Calidad de datos	Lectura	dataQualityRuleset*		
GetDataQualityRuleset	Otorga permiso para recuperar un conjunto de reglas de Calidad de datos	Lectura	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	Otorga permiso para recuperar una ejecución de recomendación de regla de Calidad de datos	Lectura	dataQualityRuleset*		
GetDatabase	Concede permiso para recuperar una base de datos	Read	database*		
			rootcatalog*		
			catalog		
GetDatabases	Concede permiso para recuperar todas las bases de datos	Read	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			rootcatalog*		
			catalog		
GetDataflowGraph	Concede permiso para transformar un script en un gráfico acíclico dirigido (DAG)	Read			
GetDevEndpoint	Concede permiso para recuperar un punto de conexión de desarrollo	Read	devendpoint*		
GetDevEndpoints	Concede permiso para recuperar todos los puntos de enlace de desarrollo	Lectura			
GetEntityRecords	Otorga permiso para previsualizar los registros de las entidades en Glue	Lectura	catalog*		
			connection		
GetEnvironment	Concede permiso para obtener detalles de entorno para SparkUI	Administración de permisos			
GetExecutors	Concede permiso para obtener ejecutores para SparkUI	Administración de permisos			
GetExecutorsThreads	Concede permiso para obtener subprocesos ejecutores para SparkUI	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGeneratedCode	Transforma un gráfico acíclico dirigido (DAG) en código	Lectura			
GetIntegrationResourceProperty	Otorga permiso para recuperar la propiedad del recurso de integración	Lectura	catalog*		
			connection*		
			database*		
GetIntegrationTableProperties	Otorga permiso para recuperar las propiedades de la tabla de integración	Lectura	catalog*		
			connection*		
			database*		
GetJob	Concede permiso para recuperar un trabajo	Read	job*		
GetJobBookmark	Concede permiso para recuperar un marcador de trabajo	Read			
GetJobRun	Concede permiso para recuperar una ejecución de trabajo	Read	job*		
GetJobRuns	Concede permiso para recuperar todas las ejecuciones de trabajo de un trabajo	Lectura	job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetJobUpgradeAnalysis	Otorga permiso para recuperar un análisis de actualización para un trabajo	Lectura	job*		
GetJobs	Concede permiso para recuperar todos los trabajos actuales	Lectura			
GetLogParsingStatus	Concede permiso para obtener el estado de análisis de registros para SparkUI	Administración de permisos			
GetMLTaskRun	Concede permiso para recuperar una ML Task Run	Read	mlTransform*		
GetMLTaskRuns	Concede permiso para recuperar todas las ML Task Run	List	mlTransform*		
GetMLTransform	Concede permiso para recuperar una transformación ML	Read	mlTransform*		
GetMLTransforms	Concede permiso para recuperar todas las transformaciones ML	List	mlTransform*		
GetMapping	Concede permiso para crear una asignación	Lectura			
GetNotebookInstanceStatus	Otorga permiso para recuperar el estado de la sesión de un bloc de notas de Glue Studio	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPartition	Concede permiso para recuperar una partición	Lectura	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitionIndexes	Concede permiso para recuperar las indexaciones de las particiones de una tabla	Lectura	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitions	Concede permiso para recuperar las particiones de una tabla	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetPlan	Concede permiso para recuperar una asignación para un script	Lectura			
GetQueries	Concede permiso para obtener consultas para SparkUI	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQuery	Concede permiso para obtener una consulta específica para SparkUI	Administración de permisos			
GetRecipeAction	Concede permiso para obtener el resultado de una instrucción de receta de preparación de datos	Administración de permisos			
GetRegistry	Concede permiso para recuperar un registro de esquemas	Read	registry*		
GetResourcePolicies	Concede permiso para recuperar políticas de recursos	Read	rootcatalog*		
GetResourcePolicy	Concede permiso para recuperar una política de recursos.	Read	rootcatalog*		
GetSchema	Concede permiso para recuperar un contenedor de esquemas	Read	registry* schema*		
GetSchemaByDefinition	Concede permiso para recuperar una versión de esquema basada en la definición de esquema	Read	registry* schema*		
GetSchemaVersion	Concede permiso para recuperar una versión de esquema	Read	registry schema		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSchemaVersionsDiff	Concede permiso para comparar dos versiones de esquema en el registro de esquemas	Read	registry* schema*		
GetSecurityConfiguration	Concede permiso para recuperar una configuración de seguridad	Read			
GetSecurityConfigurations	Concede permiso para recuperar una o varias configuraciones de seguridad	Lectura			
GetSession	Concede permiso para recuperar una sesión interactiva	Lectura	session*		
GetStage	Concede permiso para obtener una etapa para SparkUI	Administración de permisos			
GetStageAttempt	Concede permiso para obtener un intento de etapa para SparkUI	Administración de permisos			
GetStageAttemptTaskList	Concede permiso para obtener la lista de tareas para un intento de etapa para SparkUI	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetStageAttemptTaskSummary	Concede permiso para obtener el resumen de tareas para un intento de etapa para SparkUI	Administración de permisos			
GetStageFiles	Concede permiso para obtener archivos de etapa para SparkUI	Administración de permisos			
GetStages	Concede permiso para obtener etapas para SparkUI	Administración de permisos			
GetStatement	Concede permiso para recuperar resultados e información sobre una instrucción en una sesión interactiva	Lectura	session*		
GetStorage	Concede permiso para obtener detalles de almacenamiento para SparkUI	Administración de permisos			
GetStorageUnit	Concede permiso para obtener detalles de unidades de almacenamiento para SparkUI	Administración de permisos			
GetTable	Concede permiso para recuperar una tabla	Lectura	database*		
			rootcatalog*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			catalog		
GetTableOptimizer	Concede permiso para devolver la configuración de todos los optimizadores asociados a una tabla especificada	Lectura	database*		glue:GetTable
			rootcatalog*		
			table*		
GetTableVersion	Concede permiso para recuperar una versión de una tabla	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableVersions	Concede permiso para recuperar una lista de versiones de una tabla	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTables	Concede permiso para recuperar las tablas en una base de datos	Read	database*		
			rootcatalog*		
			table*		
			catalog		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTags	Concede permiso para recuperar todas las etiquetas asociadas a un recurso	Read	blueprint		
			crawler		
			customEntityType		
			devendpoint		
			job		
			trigger		
			usageProfile		
			workflow		
GetTrigger	Concede permiso para recuperar un disparador	Read	trigger*		
GetTriggers	Concede permiso para recuperar los disparadores asociados a un trabajo	Lectura			
GetUsageProfile	Concede permiso para recuperar un perfil de uso	Lectura	usageProfile*		
GetUserDefinedFunction	Concede permiso para recuperar una definición de función	Lectura	database*		
			rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			userdefinedfunction*		
			catalog		
GetUserDefinedFunctions	Concede permiso para recuperar varias definiciones de funciones	Read	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetWorkflow	Concede permiso para recuperar un flujo de trabajo	Read	workflow*		
GetWorkflowRun	Concede permiso para recuperar una ejecución de flujo de trabajo	Read	workflow*		
GetWorkflowRunProperties	Concede permiso para recuperar las propiedades de ejecución de flujo de trabajo	Read	workflow*		
GetWorkflowRuns	Concede permiso para recuperar todas las ejecuciones de un flujo de trabajo.	Lectura	workflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GlueNotebookAuthorize	Otorga permiso para acceder a los blocs de notas de Glue Studio	Administración de permisos			
GlueNotebookRefreshCredentials	Otorga permiso para actualizar las credenciales de los blocs de notas de Glue Studio	Administración de permisos			
ImportCatalogToGlue	Otorga permiso para importar un catálogo de datos de Athena a Glue AWS	Escritura	rootcatalog*		
ListBlueprints	Concede permiso para recuperar todos los esquemas	Enumeración			
ListColumnStatisticsTaskRuns	Concede permiso para mostrar todos los identificadores de ejecución de las estadísticas de columnas que se han ejecutado para la cuenta	Lectura			
ListConnectionTypes	Concede permiso para enumerar tipos de conexión en Glue Studio	Administración de permisos			
ListCrawlers	Concede permiso para recuperar todos los rastreadores.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCrawls	Concede permiso para recuperar el historial de ejecuciones de rastreo de un rastreador	Enumeración	crawler*		
ListCustomEntityTypes	Concede permiso para recuperar todos los tipos de entidad personalizados	Enumeración			
ListDataQualityResults	Otorga permiso para recuperar todos los resultados de Calidad de datos	Enumeración	dataQualityRuleset*		
ListDataQualityRuleRecommendationRuns	Otorga permiso para recuperar todas las ejecuciones de recomendación de reglas de Calidad de datos	Enumeración	dataQualityRuleset*		
ListDataQualityRulesetEvaluationRuns	Otorga permiso para recuperar todas las ejecuciones de recomendación de reglas de Calidad de datos	Enumeración	dataQualityRuleset*		
ListDataQualityRulesets	Otorga permiso para recuperar una lista de conjuntos de reglas de Calidad de datos	Enumeración	dataQualityRuleset*		
ListDevEndpoints	Otorga permiso para recuperar todos los puntos de enlace de desarrollo.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntities	Concede permiso para enumerar entidades en Glue Studio	Administración de permisos	connection*		
			rootcatalog*		
ListJobUpgradeAnalyses	Otorga permiso para enumerar los análisis de actualización de un trabajo	Enumeración	job*		
ListJobs	Otorga permiso para recuperar todos los trabajos actuales.	List			
ListMLTransforms	Otorga permiso para recuperar todas las transformaciones ML.	List	mlTransform*		
ListRegistries	Concede permiso para recuperar una lista de registros de esquemas	List			
ListSchemaVersions	Concede permiso para recuperar una lista de versiones de esquema	List	registry*		
			schema*		
ListSchemas	Concede permiso para recuperar una lista de contenedores de esquemas	Enumeración	registry		
ListSessions	Concede permiso para recuperar una lista de sesiones interactivas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStatements	Concede permiso para recuperar una lista de instrucciones de una sesión interactiva	Enumeración	session*		
ListTableOptimizerRuns	Concede permiso para mostrar el historial de las ejecuciones anteriores del optimizador para una tabla específica	Enumeración	database*		glue:GetTable
			rootcatalog*		
			table*		
ListTriggers	Concede permiso para recuperar todos los disparadores	Enumeración			
ListUsageProfiles	Concede permiso para recuperar una lista de perfiles de uso	Enumeración			
ListWorkflows	Concede permiso para recuperar todos los flujos de trabajo	Enumeración			
ModifyIntegration	Otorga permiso para modificar una integración sin ETL	Escritura	integration*		
				aws:ResourceTag/${TagKey}	
NotifyEvent	Concede permiso para notificar un evento al flujo de trabajo controlado por eventos	Escritura	workflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PassConnection [solo permiso]	Otorga permiso para pasar el nombre de la conexión adhesiva en las entradas APIs que lo requieran	Escritura	connection*		
PublishDataQuality [solo permiso]	Otorga permiso para publicar resultados de Calidad de datos	Escritura	dataQualityRuleset*		
PutDataCatalogEncryptionSettings	Concede permiso para actualizar la configuración de cifrado de catálogos	Escritura	rootcatalog*		
PutDataQualityProfileAnnotation	Concede permiso para anotar todos los puntos de datos de un perfil	Escritura	dataQualityRuleset*		
			job*		
PutDataQualityStatisticAnnotation	Concede permiso para anotar puntos de datos a lo largo del tiempo para una estadística específica de calidad de datos	Escritura	dataQualityRuleset*		
			job*		
PutResourcePolicy	Concede permiso para actualizar una política de recursos	Permissions management	rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutSchemaVersionMetadata	Concede permiso para agregar metadatos a la versión de esquema	Write	registry		
			schema		
PutWorkflowRunProperties	Concede permiso para actualizar las propiedades de ejecución de flujo de trabajo	Write	workflow*		
QuerySchemaVersionMetadata	Concede permiso para buscar metadatos para una versión de esquema	Enumeración	registry		
			schema		
RefreshOAuth2Tokens	Concede permiso para actualizar los tokens OAuth2 de la conexión durante la ejecución del trabajo	Administración de permisos	connection*		
			rootcatalog*		
RegisterSchemaVersion	Concede permiso para crear una nueva versión de esquema	Write	registry*		
			schema*		
RemoveSchemaVersionMetadata	Concede permiso para eliminar metadatos de la versión de esquema	Escritura	registry		
			schema		
RequestLogParsing	Concede permiso para solicitar el análisis de registros para SparkUI	Administración de permisos			
ResetJobBookmark	Concede permiso para restablecer un marcador de trabajo	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResumeWorkflowRun	Concede permiso para retomar una ejecución de flujo de trabajo	Escritura	workflow*		
RunDataPreviewStatement	Concede permiso para ejecutar una instrucción de vista previa de datos	Administración de permisos			
RunStatement	Concede permiso para ejecutar un código o una instrucción en una sesión interactiva	Escritura	session*		
SearchTables	Concede permiso para recuperar las tablas en el catálogo	Lectura	database*		
			rootcatalog*		
			table*		
			catalog		
SendFeedback	Otorga permiso para enviar comentarios sobre la experiencia de completar el pegamento en AWS Q	Escritura			
SendRecipeAction	Concede permiso para ejecutar una instrucción de receta de preparación de datos en la vista previa de los datos	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartBlueprintRun	Concede permiso para comenzar a ejecutar un esquema	Escritura	blueprint*		
StartColumnStatisticsTaskRun	Concede permiso para iniciar una ejecución para generar estadísticas de columnas para la tabla	Escritura	database*		glue:GetSecurityConfiguration glue:GetTable
			rootcatalog*		
			table*		
StartColumnStatisticsTaskRunSchedule	Otorga permiso para iniciar el cronograma de ejecución de una tarea estadística de columnas	Escritura	database*		
			rootcatalog*		
			table*		
StartCompletion	Otorga permiso para crear una solicitud de finalización en la experiencia Glue for AWS Q	Escritura			
StartCrawler	Concede permiso para iniciar un rastreador	Write	crawler*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCrawlerSchedule	Concede permiso para cambiar el estado de programación de un rastreador a SCHEDULED (PROGRAMADO)	Escritura			
StartDataQualityRuleRecommendationRun	Otorga permiso para iniciar una ejecución de recomendación de reglas de Calidad de datos	Escritura	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	Otorga permiso para iniciar una ejecución de recomendación de reglas de Calidad de datos	Escritura	dataQualityRuleset*		
StartExportLabelsTaskRun	Concede permiso para iniciar una Export Labels ML Task Run	Write	mlTransform*		
StartImportLabelsTaskRun	Concede permiso para iniciar una Import Labels ML Task Run	Write	mlTransform*		
StartJobRun	Concede permiso para comenzar a ejecutar un trabajo	Escritura	job*		
StartJobUpgradeAnalysis	Otorga permiso para empezar a ejecutar el análisis de actualización de un trabajo	Escritura	job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartMLEvaluationTaskRun	Concede permiso para iniciar una Evaluation ML Task Run	Write	mlTransform*		
StartMLLabelingSetGenerationTaskRun	Concede permiso para iniciar una Labeling Set Generation ML Task Run	Escritura	mlTransform*		
StartNotebook	Otorga permiso para iniciar los blocs de notas de Glue Studio	Administración de permisos			
StartTrigger	Concede permiso para iniciar un disparador	Write	trigger*		
StartWorkflowRun	Concede permiso para comenzar a ejecutar un flujo de trabajo	Escritura	workflow*		
StopColumnStatisticsTaskRun	Concede permiso para detener la ejecución de estadísticas de columnas	Escritura	database*		
			rootcatalog*		
			table*		
StopColumnStatisticsTaskRunSchedule	Otorga permiso para detener la programación de ejecución de una tarea estadística de columnas	Escritura	database*		
			rootcatalog*		
			table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopCrawler	Concede permiso para detener un rastreador en ejecución	Write	crawler*		
StopCrawlerSchedule	Concede permiso para cambiar el estado de programación de un rastreador a NOT_SCHEDULED (NO PROGRAMADO)	Escritura			
StopJobUpgradeAnalysis	Otorga permiso para detener un análisis de actualización en curso de un trabajo	Escritura	job*		
StopSession	Concede permiso para detener una sesión interactiva	Escritura	session*		
StopTrigger	Concede permiso para detener un disparador	Write	trigger*		
StopWorkflowRun	Concede permiso para detener una ejecución de flujo de trabajo	Write	workflow*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	blueprint		
			connection		
			crawler		
			customEntityType		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			dataQualityRuleset		
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TerminateNotebook	Otorga permiso para terminar los blocs de notas de Glue Studio	Administración de permisos			
TestConnection	Concede permiso para probar la conexión en Glue Studio	Administración de permisos			
UntagResource	Concede permiso para eliminar las etiquetas asociadas a un recurso	Etiquetado	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys	
UpdateBlueprint	Concede permiso para actualizar un esquema	Escritura	blueprint*		
UpdateCatalog	Otorga permiso para actualizar un catálogo	Escritura	rootcatalog*		
			catalog		
UpdateClassifier	Concede permiso para actualizar un clasificador	Escritura			
UpdateColumnStatisticsForPartition	Concede permiso para actualizar las estadísticas de partición de las columnas	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsForTable	Concede permiso para actualizar las estadísticas de tabla de las columnas	Escritura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsTaskSettings	Otorga permiso para actualizar la configuración de una tarea de estadísticas de columnas	Escritura	database*		
			rootcatalog*		
			table*		
UpdateConnection	Concede permiso para actualizar una conexión.	Write	connection*		
			rootcatalog*		
UpdateCrawler	Concede permiso para actualizar un rastreador	Write	crawler*		
UpdateCrawlerSchedule	Concede permiso para actualizar la programación de un rastreador	Escritura			
UpdateDataQualityRuleset	Otorga permiso para actualizar un conjunto de reglas de Calidad de datos	Escritura	dataQualityRuleset*		
UpdateDatabase	Concede permiso para actualizar una base de datos	Write	database*		
			rootcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			catalog		
UpdateDevEndpoint	Concede permiso para actualizar un punto de conexión de desarrollo	Escritura	devendpoint*		
UpdateIntegrationResourceProperty	Otorga permiso para actualizar la propiedad del recurso de integración	Escritura	catalog*		
			connection*		
			database*		
UpdateIntegrationTableProperties	Otorga permiso para actualizar las propiedades de la tabla de integración	Escritura	catalog*		
			connection*		
			database*		
UpdateJob	Concede permiso para actualizar un trabajo.	Escritura	job*		
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
UpdateJobFromSourceControl	Otorga permiso para actualizar un trabajo desde un proveedor de control fuente	Escritura	job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMLTransform	Concede permiso para actualizar una transformación ML	Write	mlTransform*		
UpdatePartition	Concede permiso para actualizar una partición	Write	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateRegistry	Concede permiso para actualizar un registro de esquemas	Write	registry*		
UpdateSchema	Concede permiso para actualizar un contenedor de esquemas	Escritura	registry*		
			schema*		
UpdateSourceControlFromJob	Otorga permiso para actualizar un proveedor de control fuente de un trabajo	Escritura	job*		
UpdateTable	Concede permiso para actualizar una tabla	Escritura	database*		
			rootcatalog*		
			table*		
			catalog		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTableOptimizer	Concede permiso para actualizar la configuración de un optimizador de existente	Escritura	database*		glue:GetTable
			rootcatalog*		
			table*		
UpdateTrigger	Concede permiso para actualizar un disparador	Escritura	trigger*		
UpdateUsageProfile	Concede permiso para actualizar un perfil de uso	Escritura	usageProfile*		
UpdateUserDefinedFunction	Concede permiso para actualizar una definición de función	Write	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
UpdateWorkflow	Concede permiso para actualizar un flujo de trabajo	Escritura	workflow*		
UpgradeJob	Otorga permiso para actualizar un trabajo a la versión más reciente	Escritura	job*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UseGlueStudio	Otorga permiso para usar Glue Studio y acceder a su interior APIs	Administración de permisos			
UseMLTransforms [solo permiso]	Concede permiso para utilizar una transformación ML desde un script de ETL de Glue	Write	mlTransform*		

Tipos de recursos definidos por AWS Glue

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
rootcatalog	`arn:${Partition}:glue:${Region}:${Account}:catalog`	
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}`	
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	
table	`arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}`	

Tipos de recurso	ARN	Claves de condición
tableversion	arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}	
connection	arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}	aws:ResourceTag/${TagKey}
userdefinedfunction	arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}	
devendpoint	arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:glue:${Region}:${Account}:job/${JobName}	aws:ResourceTag/${TagKey}
trigger	arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}	aws:ResourceTag/${TagKey}
crawler	arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:glue:${Region}:${Account}:blueprint/${BlueprintName}	aws:ResourceTag/${TagKey}
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:glue:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
schema	arn:${Partition}:glue:${Region}:${Account}:schema/${SchemaName}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:glue:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
usageProfile	arn:${Partition}:glue:${Region}:${Account}:usageProfile/${UsageProfileId}	aws:ResourceTag/${TagKey}
dataQualityRuleset	arn:${Partition}:glue:${Region}:${Account}:dataQualityRuleset/${RulesetName}	aws:ResourceTag/${TagKey}
customEntityType	arn:${Partition}:glue:${Region}:${Account}:customEntityType/${CustomEntityTypeId}	aws:ResourceTag/${TagKey}
completion	arn:${Partition}:glue:${Region}:${Account}:completion/${CompletionId}	
integration	arn:${Partition}:glue:${Region}:${Account}:integration:${IntegrationId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Glue

AWS Glue define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
glue:CredentialIssuingService	Filtra el acceso por el servicio desde el que se emiten las credenciales de la solicitud	Cadena
glue:EnabledForRedshiftAutoDiscovery	Filtra el acceso según la presencia de la clave configurada para la política basada en la identidad del rol	Bool
glue:RoleAssumedBy	Filtra el acceso por el servicio desde el que se obtienen las credenciales de la solicitud asumiendo el rol de cliente	Cadena
glue:SecurityGroupIds	Filtra el acceso según el ID de los grupos de seguridad configurados para el trabajo Glue	ArrayOfString
glue:SubnetIds	Filtra el acceso según el ID de las subredes configuradas para el trabajo Glue	ArrayOfString
glue:VpcIds	Filtra el acceso según el ID de la VPC configurada para el trabajo Glue.	ArrayOfString

Acciones, recursos y claves de condición de AWS Glue DataBrew

AWS Glue DataBrew (prefijo de servicio:`databrew`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Glue DataBrew
- Tipos de recursos definidos por AWS Glue DataBrew
- Claves de estado para AWS Glue DataBrew

Acciones definidas por AWS Glue DataBrew

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDeleteRecipeVersion	Otorga permiso para eliminar una o varias versiones de una receta.	Write	Recipe*		
CreateDataset	Concede permiso para crear un conjunto de datos	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
CreateProfileJob	Otorga permiso para crear un trabajo de perfil.	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProject	Concede permiso para crear un proyecto	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRecipe	Otorga permiso para crear una receta.	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecipeJob	Otorga permiso para crear un trabajo de receta.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRuleset	Otorga permiso para crear un conjunto de reglas.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSchedule	Otorga permiso para crear una programación.	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteDataset	Concede permiso para eliminar un conjunto de datos	Write	Dataset*		
DeleteJob	Concede permiso para eliminar un trabajo.	Write	Job*		
DeleteProject	Concede permiso para eliminar un proyecto	Write	Project*		
DeleteRecipeVersion	Otorga permiso para eliminar una versión de receta.	Escritura	Recipe*		
DeleteRuleset	Otorga permiso para eliminar un conjunto de reglas.	Escritura	Ruleset*		
DeleteSchedule	Otorga permiso para eliminar una programación.	Write	Schedule*		
DescribeDataset	Otorga permiso para ver detalles de un conjunto de datos.	Read	Dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeJob	Otorga permiso para ver detalles de un trabajo.	Read	Job*		
DescribeJobRun	Otorga permiso para ver detalles de un trabajo ejecutado para un trabajo determinado	Read	Job*		
DescribeProject	Otorga permiso para ver detalles de un proyecto.	Read	Project*		
DescribeRecipe	Otorga permiso para ver detalles de una receta.	Lectura	Recipe*		
DescribeRuleset	Otorga permiso para ver detalles de un conjunto de reglas.	Lectura	Ruleset*		
DescribeSchedule	Otorga permiso para ver detalles de una programación.	Read	Schedule*		
ListDatasets	Otorga permiso para enumerar los conjuntos de datos en su cuenta.	Read			
ListJobRuns	Otorga permiso para enumerar las ejecuciones de trabajo para un trabajo determinado.	Read	Job*		
ListJobs	Otorga permiso para enumerar los trabajos en su cuenta.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProjects	Otorga permiso para enumerar los proyectos en su cuenta.	Read			
ListRecipeVersions	Otorga permiso para enumerar las versiones en su receta.	Read	Recipe*		
ListRecipes	Otorga permiso para enumerar las recetas en su cuenta.	Lectura			
ListRulesets	Otorga permiso para enumerar los conjuntos de reglas en su cuenta.	Lectura			
ListSchedules	Otorga permiso para enumerar las programaciones en su cuenta.	Read			
ListTagsForResource	Otorga permiso para recuperar las etiquetas asociadas a un recurso.	Read	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PublishRecipe	Otorga permiso para publicar la versión principal de una receta.	Write	Recipe*		
SendProjectSessionAction	Otorga permiso para enviar una acción a la sesión interactiva de un proyecto.	Write	Project*		
StartJobRun	Concede permiso para comenzar a ejecutar un trabajo	Write	Job*		
StartProjectSession	Otorga permiso para iniciar una sesión interactiva de un proyecto.	Write	Project*		
StopJobRun	Otorga permiso para detener la ejecución de un trabajo para un trabajo.	Write	Job*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas asociadas a un recurso	Etiquetado	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	Otorga permiso para modificar un conjunto de datos.	Write	Dataset*		
UpdateProfileJob	Otorga permiso para modificar un trabajo de perfil.	Write	Job*		
UpdateProject	Otorga permiso para modificar un proyecto.	Write	Project*		
UpdateRecipe	Otorga permiso para modificar una receta.	Write	Recipe*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRecipeJob	Otorga permiso para modificar un trabajo de una receta.	Escritura	Job*		
UpdateRuleset	Otorga permiso para modificar un conjunto de reglas.	Escritura	Ruleset*		
UpdateSchedule	Otorga permiso para modificar una programación.	Escritura	Schedule*		

Tipos de recursos definidos por AWS Glue DataBrew

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Project	`arn:${Partition}:databrew:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}
Dataset	`arn:${Partition}:databrew:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
Ruleset	`arn:${Partition}:databrew:${Region}:${Account}:ruleset/${ResourceId}`	aws:ResourceTag/${TagKey}
Recipe	`arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Job	`arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}`	aws:ResourceTag/${TagKey}
Schedule	`arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de estado para AWS Glue DataBrew

AWS Glue DataBrew define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Ground Station

AWS Ground Station (prefijo de servicio:`groundstation`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Ground Station
- Tipos de recursos definidos por AWS Ground Station
- Claves de condición para AWS Ground Station

Acciones definidas por AWS Ground Station

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelContact	Otorga permiso para cancelar un contacto	Write	Contact*		
CreateConfig	Otorga permiso para crear una configuración.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroup	Otorga permiso para crear un grupo de punto de enlace de flujo de datos.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEphemeris	Otorga permiso para crear un objeto efeméride	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMissionProfile	Otorga permiso para crear un perfil de misión.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfig	Otorga permiso para eliminar una configuración.	Write	Config*		
DeleteDataflowEndpointGroup	Otorga permiso para eliminar un grupo de puntos de enlace de flujo de datos.	Escritura	DataflowEndpointGroup*		
DeleteEphemeris	Otorga permiso para eliminar un objeto efeméride	Escritura	EphemerisItem*		
DeleteMissionProfile	Otorga permiso para eliminar un perfil de misión.	Write	MissionProfile*		
DescribeContact	Otorga permiso para describir un contacto	Lectura	Contact*		
DescribeEphemeris	Otorga permiso para describir un objeto efeméride	Lectura	EphemerisItem*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAgentConfiguration	Concede permiso para obtener la configuración de un agente	Lectura	Agent*		
GetConfig	Otorga permiso para devolver una configuración.	Read	Config*		
GetDataflowEndpointGroup	Otorga permiso para devolver un grupo de puntos de enlace fe flujo de datos.	Read	DataflowEndpointGroup*		
GetMinuteUsage	Otorga permiso para devolver el uso de minutos.	Read			
GetMissionProfile	Otorga permiso para recuperar un perfil de misión.	Read	MissionProfile*		
GetSatellite	Otorga permiso para devolver información acerca de un satélite.	Read	Satellite*		
ListConfigs	Otorga permiso para devolver una lista de configuraciones anteriores	List			
ListContacts	Otorga permiso para devolver una lista de contactos	List			
ListDataflowEndpointGroups	Otorga permiso para obtener una lista de grupos de puntos de enlace de flujo de datos.	Enumeración			
ListEphemerides	Otorga permiso para enumerar efeméride	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGroundStations	Otorga permiso para obtener una lista de estaciones terrestres.	List			
ListMissionProfiles	Otorga permiso para obtener una lista de perfiles de misión.	List			
ListSatellites	Otorga permiso para obtener una lista de satélites.	List			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	Config		
			Contact		
			DataflowEndpointGroup		
			MissionProfile		
RegisterAgent	Concede permiso para registrar un agente	Escritura			
ReserveContact	Otorga permiso para reservar un contacto	Write		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para asignar una etiqueta de recurso.	Etiquetado	Config		
			Contact		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para desasignar una etiqueta de recurso	Etiquetado	Config		
			Contact		
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAgentStatus	Concede permiso para actualizar el estado de un agente	Escritura	Agent*		
UpdateConfig	Otorga permiso para actualizar una configuración.	Escritura	Config*		
UpdateEphemeris	Otorga permiso para actualizar un objeto efeméride	Escritura	EphemerisItem*		
UpdateMissionProfile	Otorga permiso para actualizar un perfil de misión.	Write	MissionProfile*		

Tipos de recursos definidos por AWS Ground Station

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${ConfigType}/${ConfigId}`	aws:ResourceTag/${TagKey} groundstation:ConfigId

Tipos de recurso	ARN	Claves de condición
		groundstation:ConfigType
Contact	arn:${Partition}:groundstation:${Region}:${Account}:contact/${ContactId}	aws:ResourceTag/${TagKey} groundstation:ContactId
DataflowEndpointGroup	arn:${Partition}:groundstation:${Region}:${Account}:dataflow-endpoint-group/${DataflowEndpointGroupId}	aws:ResourceTag/${TagKey} groundstation:DataflowEndpointGroupId
EphemerisItem	arn:${Partition}:groundstation:${Region}:${Account}:ephemeris/${EphemerisId}	aws:ResourceTag/${TagKey} groundstation:EphemerisId
GroundStationResource	arn:${Partition}:groundstation:${Region}:${Account}:groundstation:${GroundStationId}	groundstation:GroundStationId
MissionProfile	arn:${Partition}:groundstation:${Region}:${Account}:mission-profile/${MissionProfileId}	aws:ResourceTag/${TagKey} groundstation:MissionProfileId
Satellite	arn:${Partition}:groundstation:${Region}:${Account}:satellite/${SatelliteId}	groundstation:SatelliteId
Agent	arn:${Partition}:groundstation:${Region}:${Account}:agent/${AgentId}	groundstation:AgentId

Claves de condición para AWS Ground Station

AWS Ground Station define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
groundstation:AgentId	Filtra el acceso por el ID de un agente	Cadena
groundstation:ConfigId	Filtra el acceso por ID de una configuración.	Cadena
groundstation:ConfigType	Filtra el acceso por el tipo de una configuración.	Cadena
groundstation:ContactId	Filtra el acceso por el ID de un contacto.	Cadena
groundstation:DataflowEndpointGroupId	Filtra el acceso por el ID de un grupo de puntos de enlace de flujo de datos.	Cadena

Claves de condición	Descripción	Tipo
groundstation:EphemerisId	Filtra el acceso por el ID de una efeméride	Cadena
groundstation:GroundStationId	Filtra el acceso por el ID de una estación terrestre.	Cadena
groundstation:MissionProfileId	Filtra el acceso por el ID de un perfil de misión.	Cadena
groundstation:SatelliteId	Filtra el acceso por el ID de un satélite.	Cadena

Acciones, recursos y claves de condición para Amazon GroundTruth Labeling

Amazon GroundTruth Labeling (prefijo de servicio:`groundtruthlabeling`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon GroundTruth Labeling
- Tipos de recursos definidos por Amazon GroundTruth Labeling
- Claves de estado para Amazon GroundTruth Labeling

Acciones definidas por Amazon GroundTruth Labeling

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociatePatchToManifestJob [solo permiso]	Concede permiso para asociar un archivo de parche con el archivo de manifiesto a fin de actualizar el archivo de manifiesto	Write			
CreateBatch [solo permiso]	Concede permiso para crear un lote de GT+	Escritura			
CreateIntakeForm [solo permiso]	Concede permiso para crear un formulario de ingreso	Escritura			
CreateProject [solo permiso]	Concede permiso para crear un proyecto de GT+	Escritura			
CreateWorkflowDefinition [solo permiso]	Concede permiso para crear una definición de flujo de trabajo de GT+	Escritura			
DescribeConsoleJob [solo permiso]	Otorga permiso para obtener el estado de los trabajos GroundTruthLabeling	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateLIDARPreviewTaskConfigJob [solo permiso]	Concede permiso para generar una tarea de vista previa de LiDAR	Escritura			
GetBatch [solo permiso]	Concede permiso para obtener un lote de GT+	Lectura			
GetIntakeFormStatus [solo permiso]	Concede permiso para obtener formularios de ingreso	Lectura			
ListBatches [solo permiso]	Concede permiso para enumerar lotes de GT+	Lectura			
ListDatasetObjects [solo permiso]	Concede permiso para mostrar objetos del conjunto de datos en un archivo de manifiesto	Read			
ListProjects [solo permiso]	Concede permiso para enumerar proyectos de GT+	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RunFilterOrSampleDatasetJob [solo permiso]	Concede permiso para filtrar registros de un archivo de manifiesto mediante S3 Select. Obtener entradas de muestra basadas en un muestreo aleatorio	Write			
RunGenerateManifestByCrawlingJob [solo permiso]	Concede permiso para mostrar un prefijo de S3 y crear archivos de manifiesto a partir de objetos en esa ubicación	Escritura			
RunGenerateManifestMetricsJob [solo permiso]	Concede permiso para generar métricas a partir de objetos en el manifiesto	Escritura			
UpdateBatch [solo permiso]	Concede permiso para actualizar un lote de GT+	Escritura			

Tipos de recursos definidos por Amazon GroundTruth Labeling

Amazon GroundTruth Labeling no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a Amazon GroundTruth Labeling, `"Resource": "*"` especifícalo en tu política.

Claves de estado para Amazon GroundTruth Labeling

GroundTruth El etiquetado no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de

contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de Amazon GuardDuty

Amazon GuardDuty (prefijo de servicio:`guardduty`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon GuardDuty
- Tipos de recursos definidos por Amazon GuardDuty
- Claves de estado de Amazon GuardDuty

Acciones definidas por Amazon GuardDuty

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptAdministratorInvitation	Otorga permiso para aceptar invitaciones para convertirse en una cuenta de GuardDuty miembro	Escritura			
AcceptInvitation	Otorga permiso para aceptar invitaciones para convertirse	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	en una cuenta de GuardDuty miembro				
ArchiveFindings	Otorga permiso para archivar GuardDuty las conclusiones	Escritura			
CreateDetector	Otorga permiso para crear un detector	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateFilter	Otorga permiso para crear GuardDuty filtros. Un filtro define los atributos de búsqueda y las condiciones que se utilizan para filtrar resultados	Escritura	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIPSet	Otorga permiso para crear un IPSet	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy
CreateMalwareProtectionPlan	Concede permiso para crear un nuevo plan de protección contra malware	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateMembers	Otorga permiso para crear cuentas de GuardDuty miembros, donde la cuenta utilizada para crear un miembro pasa a ser la cuenta de GuardDuty administrador	Escritura			
CreatePublishingDestination	Otorga permisos para crear un destino de publicación	Write			s3:GetObject s3:ListBucket

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSampleFindings	Otorga permiso para crear hallazgos de muestra	Escritura			
CreateThreatIntelSet	Otorga permiso de creación GuardDuty ThreatIntelSets, donde a ThreatIntelSet consiste en direcciones IP maliciosas conocidas utilizadas GuardDuty para generar hallazgos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeclineInvitations	Otorga permiso para rechazar invitaciones para convertirse en una cuenta de GuardDuty miembro	Escritura			
DeleteDetector	Otorga permiso para eliminar GuardDuty los detectores	Escritura	detector*		
DeleteFilter	Otorga permiso para eliminar GuardDuty filtros	Escritura	filter*		
DeleteIPSet	Otorga permiso para eliminar GuardDuty IPSets	Escritura	ipset*		
DeleteInvitations	Otorga permiso para eliminar las invitaciones para convertirse en una cuenta de GuardDuty miembro	Escritura			
DeleteMalwareProtectionPlan	Concede permiso para crear un nuevo plan de protección contra malware	Escritura	malwareprotectionplan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMembers	Otorga permiso para eliminar las cuentas GuardDuty de los miembros	Escritura			
DeletePublishingDestination	Otorga permisos para eliminar un destino de publicación	Escritura	publishingDestination*		
DeleteThreatIntelSet	Otorga permiso para eliminar GuardDuty ThreatIntelSets	Escritura	threatintelset*		
DescribeMalwareScans	Otorga permiso para recuperar los detalles sobre análisis de malware	Lectura			
DescribeOrganizationConfiguration	Otorga permiso para recuperar detalles sobre el administrador delegado asociado a un detector GuardDuty	Lectura			
DescribePublishingDestination	Otorga permisos para recuperar detalles sobre un destino de publicación	Lectura	publishingDestination*		
DisableOrganizationAdminAccount	Otorga permiso para deshabilitar el administrador delegado de la organización para GuardDuty	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateFromAdministratorAccount	Otorga permiso para desasociar una cuenta de GuardDuty miembro de su cuenta de administrador GuardDuty	Escritura			
DisassociateFromMasterAccount	Otorga permiso para desasociar una cuenta de GuardDuty miembro de su cuenta de administrador GuardDuty	Escritura			
DisassociateMembers	Otorga permiso para desasociar las cuentas de GuardDuty los miembros de su cuenta de administrador GuardDuty	Escritura			
EnableOrganizationAdminAccount	Otorga permiso para que un administrador delegado de la organización pueda GuardDuty	Escritura			
GetAdministratorAccount	Otorga permiso para recuperar los detalles de la cuenta de GuardDuty administrador asociada a la cuenta de un miembro	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCoverageStatistics	Otorga permiso para incluir las estadísticas de GuardDuty cobertura de Amazon para la GuardDuty cuenta especificada en una región	Lectura	detector*		
GetDetector	Otorga permiso para recuperar GuardDuty los detectores	Lectura	detector*		
GetFilter	Otorga permiso para recuperar GuardDuty filtros	Lectura	filter*		
GetFindings	Otorga permiso para recuperar GuardDuty los hallazgos	Lectura			
GetFindingsStatistics	Otorga permiso para recuperar una lista de estadísticas de GuardDuty búsqueda	Lectura			
GetIPSet	Otorga permiso para recuperar GuardDuty IPSets	Lectura	ipset*		
GetInvitationsCount	Otorga permiso para recuperar el recuento de todas GuardDuty las invitaciones enviadas a una cuenta específica, que no incluye la invitación aceptada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMalwareProtectionPlan	Concede permiso para recuperar los detalles de un plan de protección contra malware	Lectura	malwareprotectionplan*		
GetMalwareScanSettings	Otorga permiso para recuperar la configuración de análisis de malware	Lectura			
GetMasterAccount	Otorga permiso para recuperar los detalles de la cuenta de GuardDuty administrador asociada a la cuenta de un miembro	Lectura			
GetMemberDetectors	Otorga permiso para describir qué orígenes de datos están habilitados para los detectores de cuentas de miembros	Lectura			
GetMembers	Otorga permiso para recuperar las cuentas de miembro asociadas a una cuenta de administrador	Lectura			
GetOrganizationStatistics	Otorga permiso para recuperar las estadísticas de cobertura del plan de GuardDuty protección de las cuentas de los miembros en una región	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRemainingFreeTrialDays	Concede permiso para indicar el número de días restantes para cada origen de datos utilizado en el periodo de prueba gratuito	Lectura			
GetThreatIntelSet	Otorga permiso para recuperarlas GuardDuty ThreatIntelSets	Lectura	threatintelset*		
GetUsageStatistics	Otorga permiso para incluir las estadísticas de GuardDuty uso de Amazon de los últimos 30 días para el ID de detector especificado	Lectura			
InviteMembers	Otorga permiso para invitar a otras AWS cuentas a habilitar las GuardDuty y convertirse en cuentas de GuardDuty miembros	Escritura			
ListCoverage	Concede permiso para enumerar todos los detalles de un recurso para una cuenta determinada en una región	Enumeración	detector*		
ListDetectors	Otorga permiso para recuperar una lista de GuardDuty detectores	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFilters	Otorga permiso para recuperar una lista de GuardDuty filtros	Enumeración			
ListFindings	Otorga permiso para recuperar una lista de GuardDuty hallazgos	Enumeración			
ListIPSets	Otorga permiso para recuperar una lista de GuardDuty IPSets	Enumeración			
ListInvitations	Otorga permiso para recuperar una lista de todas las invitaciones de GuardDuty membresía que se enviaron a un Cuenta de AWS	Enumeración			
ListMalwareProtectionPlans	Concede permiso para recuperar una lista de planes de protección contra malware	Enumeración			
ListMembers	Otorga permiso para recuperar una lista de cuentas de GuardDuty miembros asociadas a una cuenta de administrador	Enumeración			
ListOrganizationAdminAccounts	Otorga permiso para incluir detalles sobre el administrador delegado de la organización para GuardDuty	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPublishingDestinations	Otorga permisos para recuperar una lista de destinos de publicación	Enumeración			
ListTagsForResource	Otorga permiso para recuperar una lista de etiquetas asociadas a un recurso GuardDuty	Lectura	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		
ListThreatIntelSets	Otorga permiso para recuperar una lista de GuardDuty ThreatIntelSets	Enumeración			
SendSecurityTelemetry	Otorga permiso para enviar telemetría de seguridad a una GuardDuty cuenta específica de una región	Escritura			
StartMalwareScan	Concede permiso para iniciar un nuevo análisis de malware	Escritura			
StartMonitoringMembers	Otorga permiso a una cuenta de GuardDuty administrador para supervisar los resultados de las cuentas de los miembros GuardDuty	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopMonitoringMembers	Otorga permiso para desactivar los resultados de monitoreo de las cuentas de miembro	Escritura			
TagResource	Otorga permiso para añadir etiquetas a un GuardDuty recurso	Etiquetado	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveFindings	Otorga permiso para desarchivar los hallazgos GuardDuty	Escritura			
UntagResource	Otorga permiso para eliminar etiquetas de un recurso GuardDuty	Etiquetado	detector		
			filter		
			ipset		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			malwareprotectionplan		
			threatintelset		
				aws:TagKeys	
UpdateDetector	Otorga permiso para actualizar GuardDuty los detectores	Escritura	detector*		
UpdateFilter	Otorga permiso para actualizar GuardDuty los filtros	Escritura	filter*		
UpdateFindingsFeedback	Otorga permiso para actualizar los comentarios sobre los GuardDuty hallazgos para marcarlos como útiles o no útiles	Escritura			
UpdateIPSet	Otorga permiso para actualizar GuardDuty IPSets	Escritura	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareProtectionPlan	Concede permiso para actualizar el plan de protección contra malware	Escritura	malwareprotectionplan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMalwareScanSettings	Otorga permiso para actualizar la configuración de análisis de malware	Escritura			
UpdateMemberDetectors	Otorga permiso para actualizar qué orígenes de datos están habilitados para los detectores de cuentas de miembros	Escritura			
UpdateOrganizationConfiguration	Otorga permiso para actualizar la configuración del administrador delegado asociada a un detector GuardDuty	Escritura			
UpdatePublishingDestination	Otorga permisos para actualizar un destino de publicación	Escritura	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatIntelSet	Otorga permiso para actualizar el GuardDuty ThreatIntelSets	Escritura	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy

Tipos de recursos definidos por Amazon GuardDuty

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey}
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}`	aws:ResourceTag/${TagKey}
threatintelset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}`	aws:ResourceTag/${TagKey}
publishingDestination	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingDestination/${PublishingDestinationId}`	
malwareprotectionplan	`arn:${Partition}:guardduty:${Region}:${Account}:malware-protection-plan/${MalwareProtectionPlanId}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon GuardDuty

Amazon GuardDuty define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de estado para AWS Health APIs and Notifications

AWS Health APIs and Notifications (prefijo de servicio:`health`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Health APIs and Notifications
- Tipos de recursos definidos por AWS Health APIs and Notifications
- Claves de condición para AWS Health APIs and Notifications

Acciones definidas por AWS Health APIs and Notifications

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAffectedAccountsForOrganization	Otorga permiso para obtener una lista de cuentas que se han visto afectadas por los eventos especificados en la organización	Lectura			organizations:ListAccounts
DescribeAffectedEntities	Otorga permiso para obtener una lista de entidades que se han visto afectadas por los eventos especificados	Lectura	event*		
				health:eventTypeCode health:service	
DescribeAffectedEntitiesForOrganization	Otorga permiso para obtener una lista de entidades que se han visto afectadas por los eventos y cuentas especificados en la organización	Lectura			organizations:ListAccounts
DescribeEntityAggregates	Otorga permiso para devolver el número de entidades que se ven afectadas por cada uno de los eventos especificados	Lectura			
DescribeEntityAggregatesForOrganization	Otorga permiso para devolver el número de entidades que se ven afectadas por cada uno	Lectura			organizations:ListAccounts

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de los eventos especificados en una organización				
DescribeEventAggregates	Otorga permiso para devolver el número de eventos de cada tipo de evento (problema, cambio programado y notificación de cuenta)	Lectura			
DescribeEventDetails	Otorga permiso para devolver información detallada sobre uno o varios eventos especificados	Lectura	event*		
				health:eventTypeCode health:service	
DescribeEventDetailsForOrganization	Otorga permiso para devolver información detallada sobre uno o más eventos especificados de las cuentas proporcionadas en la organización	Lectura			organizations:ListAccounts
DescribeEventTypes	Otorga permiso para devolver los tipos de eventos que cumplen los criterios de filtro especificados	Lectura			
DescribeEvents	Otorga permiso para devolver información sobre los eventos que cumplen con los criterios de filtro especificados	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEventsForOrganization	Otorga permiso para devolver información sobre los eventos que cumplen con los criterios de filtro especificados en la organización	Lectura			organizations:ListAccounts
DescribeHealthServiceStatusForOrganization	Otorga permiso para devolver el estado de la activación o desactivación de la característica Vista organizativa	Lectura			organizations:ListAccounts
DisableHealthServiceAccessForOrganization	Otorga permiso para desactivar la característica de Vista organizativa	Administración de permisos			organizations:DisableAWSServiceAccess organizations:ListAccounts

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableHealthServiceAccessForOrganization	Otorga permiso para habilitar la característica de Vista organizativa	Administración de permisos			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

Tipos de recursos definidos por AWS Health APIs and Notifications

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

Claves de condición para AWS Health APIs and Notifications

AWS Health APIs and Notifications define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
health:eventTypeCode	Filtra el acceso según el tipo de evento	Cadena
health:service	Filtra el acceso según el servicio afectado	Cadena

Acciones, recursos y claves de condición para AWS HealthImaging

AWS HealthImaging (prefijo de servicio:`medical-imaging`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS HealthImaging
- Tipos de recursos definidos por AWS HealthImaging
- Claves de condición de AWS HealthImaging

Acciones definidas por AWS HealthImaging

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CopyImageSet	Otorga permiso para copiar un conjunto de imágenes	Escritura	datastore*		
			imageset*		
CreateDatastore	Otorga permiso para crear un almacén de datos para ingerir datos de imágenes	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatastore	Otorga permiso para eliminar un almacén de datos	Escritura	datastore*		
DeleteImageSet	Otorga permiso para eliminar un conjunto de imágenes	Escritura	datastore*		
			imageset*		
GetDICOMImportJob	Otorga permiso para obtener las propiedades de un trabajo de importación	Lectura	datastore*		
GetDICOMInstance	Concede permiso para obtener una instancia DICOM en formato DCM	Lectura	datastore*		
GetDICOMInstanceFrames	Concede permiso para obtener fotogramas de instancias DICOM en el	Lectura	datastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	formato solicitado por el cliente				
GetDICOMInstanceMetadata	Concede permiso para obtener metadatos de instancias DICOM en formato JSON de DICOM	Lectura	datastore*		
GetDICOMSeriesMetadata	Otorga permiso para recuperar los metadatos de todas las instancias DICOM que pertenezcan a una serie DICOM determinada en formato DICOM JSON	Lectura	datastore*		
GetDatastore	Otorga permiso para obtener las propiedades del almacén de datos	Lectura	datastore*		
GetImageFrame	Otorga permiso para obtener las propiedades del marco de la imagen	Lectura	datastore*		
			imageset*		
GetImageSet	Otorga permiso para obtener propiedades del conjunto de imágenes	Lectura	datastore*		
			imageset*		
GetImageSetMetadata	Otorga permiso para obtener propiedades de metadatos del conjunto de imágenes	Lectura	datastore*		
			imageset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDICOMImportJobs	Otorga permiso para enumerar trabajos de importación para un almacén de datos	Enumeración	datastore*		
ListDatastores	Otorga permiso para enumerar almacenes de datos	Enumeración			
ListImageSetVersions	Otorga permiso para enumerar versiones de un conjunto de imágenes	Enumeración	datastore*		
			imageset*		
ListTagsForResource	Otorga permiso para enumerar etiquetas para un recurso de imágenes médicas	Enumeración	datastore		
			imageset		
SearchDICOMInstances	Otorga permiso para buscar instancias de dicom que devuelvan datos en formato DICOM JSON	Lectura	datastore*		
SearchDICOMSeries	Otorga permiso para buscar series dicom que devuelvan datos en formato DICOM JSON	Lectura	datastore*		
SearchDICOMStudies	Otorga permiso para buscar estudios dicom que devuelvan datos en formato DICOM JSON	Lectura	datastore*		
SearchImageSets	Otorga permiso para buscar conjuntos de imágenes	Lectura	datastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDICOMImportJob	Otorga permiso para iniciar un trabajo de importación DICOM	Escritura	datastore*		
TagResource	Otorga permiso para agregar etiquetas a un recurso de imágenes médicas	Etiquetado	datastore		
			imageset		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de imágenes médicas	Etiquetado	datastore		
			imageset		
				aws:TagKeys	
UpdateImageSetMetadata	Otorga permiso para actualizar las propiedades de metadatos del conjunto de imágenes	Escritura	datastore*		
			imageset*		

Tipos de recursos definidos por AWS HealthImaging

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
datastore	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}`	aws:ResourceTag/${TagKey}
imageset	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}/imageset/${ImageSetId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS HealthImaging

AWS HealthImaging define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS HealthLake

AWS HealthLake (prefijo de servicio:`healthlake`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS HealthLake
- Tipos de recursos definidos por AWS HealthLake
- Claves de condición de AWS HealthLake

Acciones definidas por AWS HealthLake

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelFHIRExportJobWithDelete	Concede permiso para cancelar un trabajo de exportación FHIR en curso con Eliminar	Escritura	datastore*		
CreateFHIRDatastore	Otorga permiso para crear un almacén de datos que pueda incorporar y exportar datos de FHIR	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResource	Otorga permiso para crear un recurso	Write	datastore*		
DeleteFHIRDatastore	Otorga permiso para eliminar un almacén de datos	Write	datastore*		
DeleteResource	Otorga permiso para eliminar un recurso	Write	datastore*		
DescribeFHIRDatastore	Otorga permiso para obtener las propiedades asociadas al almacén de datos de FHIR, incluido el ID, ARN, nombre y estado del almacén de datos, creado en, la versión del tipo de almacén de datos y el punto de enlace del almacén de datos	Read	datastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFHIRExportJob	Otorga permiso para mostrar las propiedades de un trabajo de exportación de FHIR, incluido el ID, ARN, nombre y estado del almacén de datos	Lectura	datastore*		
DescribeFHIRExportJobWithGet	Concede permiso para mostrar las propiedades de un trabajo de exportación FHIR, incluido el ID, ARN, nombre y el estado del almacén de datos con Obtener	Lectura	datastore*		
DescribeFHIRImportJob	Otorga permiso para mostrar las propiedades de un trabajo de importación de FHIR, incluido el ID, ARN, nombre y estado del almacén de datos	Read	datastore*		
GetCapabilities	Otorga permiso para obtener las capacidades de un almacén de datos FHIR	Lectura	datastore*		
GetExportedFile	Otorga permiso para acceder a los archivos exportados desde un trabajo de exportación de FHIR iniciado con Get	Lectura	datastore*		
GetHistoryByResourceId	Otorga permiso para leer el historial de recursos	Lectura	datastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFHIRDatastores	Concede permiso para enumerar todos los almacenes de datos FHIR que están en la cuenta del usuario, independientemente del estado del almacén de datos	Enumeración			
ListFHIRExportJobs	Otorga permiso para obtener una lista de trabajos de exportación para el almacén de datos especificado	List	datastore*		
ListFHIRImportJobs	Otorga permiso para obtener una lista de trabajos de importación para el almacén de datos especificado	List	datastore*		
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas para el almacén de datos especificado	Enumeración	datastore		
ProcessBundle	Otorga permiso para agrupar varias operaciones de recursos	Escritura	datastore*		
ReadResource	Otorga permiso para leer el recurso	Lectura	datastore*		
SearchEverything	Concede permiso para buscar todos los recursos relacionados con un paciente	Lectura	datastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchWithGet	Otorga permiso para buscar recursos con el método GET	Read	datastore*		
SearchWithPost	Otorga permiso para buscar recursos con el método POST	Read	datastore*		
StartFHIRExportJob	Otorga permiso para iniciar un trabajo de exportación de FHIR	Escritura	datastore*		
StartFHIRExportJobWithGet	Otorga permiso para iniciar un trabajo de exportación de FHIR con Get	Escritura	datastore*		
StartFHIRExportJobWithPost	Concede permiso para iniciar un trabajo de exportación FHIR con Publicar	Escritura	datastore*		
StartFHIRImportJob	Otorga permiso para iniciar un trabajo de importación de FHIR	Write	datastore*		
TagResource	Otorga permiso para agregar etiquetas a un almacén de datos	Etiquetado	datastore	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para quitar las etiquetas asociadas a un almacén de datos	Etiquetado	datastore		
				aws:TagKeys	
UpdateResource	Otorga permiso para actualizar el recurso	Escritura	datastore *		
VersionReadResource	Otorga permiso para leer la versión de un recurso	Lectura	datastore *		

Tipos de recursos definidos por AWS HealthLake

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
datastore	`arn:${Partition}:healthlake:${Region}:${Account}:datastore/fhir/${DatastoreId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS HealthLake

AWS HealthLake define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las

que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la presencia de los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS HealthOmics

AWS HealthOmics (prefijo de servicio:`omics`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS HealthOmics
- Tipos de recursos definidos por AWS HealthOmics
- Claves de condición de AWS HealthOmics

Acciones definidas por AWS HealthOmics

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AbortMultipartReadSetUpload	Concede permiso para anular cargas de conjuntos de lectura multiparte	Escritura	sequenceStore*		
AcceptShare	Otorga permiso para aceptar un recurso compartido	Escritura			
BatchDeleteReadSet	Otorga permiso para eliminar por lotes conjuntos de lectura en el almacén de secuencias determinado	Escritura	sequenceStore*		
CancelAnnotationImportJob	Otorga permiso para cancelar un trabajo de importación de anotaciones	Escritura			
CancelRun	Otorga permiso para cancelar la ejecución de un flujo de trabajo y detener todas las tareas del flujo de trabajo	Escritura	run*		
CancelVariantImportJob	Otorga permiso para cancelar un trabajo de importación de variantes	Escritura			
CompleteMultipartReadSetUpload	Concede permiso para completar una carga de conjunto de lectura multiparte	Escritura	sequenceStore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAnnotationStore	Otorga permiso para crear un almacén de anotaciones	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnnotationStoreVersion	Otorga permiso para crear una versión en un almacén de anotaciones	Escritura	AnnotationStore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultipartReadSetUpload	Concede permiso para crear una carga de conjunto de lectura multiparte	Escritura	sequenceStore*		
CreateReferenceStore	Otorga permiso para crear un almacén de referencias	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunCache	Otorga permiso para crear una nueva caché de ejecución de flujos de trabajo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRunGroup	Otorga permiso para crear un nuevo grupo de ejecuciones de flujos de trabajo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSequenceStore	Otorga permiso para crear un almacén de secuencias	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateShare	Otorga permiso para crear un recurso compartido	Escritura			
CreateVariantStore	Otorga permiso para crear un almacén de variantes	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflow	Otorga permiso para crear un nuevo flujo de trabajo con una definición de flujo de trabajo y una plantilla de parámetros de flujo de trabajo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateWorkflowVersion	Otorga permiso para crear una nueva versión del flujo de trabajo con una definición del flujo de trabajo y una plantilla de parámetros del flujo de trabajo	Escritura	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnnotationStore	Otorga permiso para eliminar un almacén de anotaciones	Escritura	AnnotationStore*		
DeleteAnnotationStoreVersions	Otorga permiso para eliminar versiones en un almacén de anotaciones	Escritura	AnnotationStore*		
			AnnotationStoreVersion*		
DeleteReference	Otorga permiso para eliminar una referencia del almacén de referencias determinado	Escritura	reference*		
			referenceStore*		
DeleteReferenceStore	Otorga permiso para eliminar un almacén de referencias	Escritura	referenceStore*		
DeleteRun	Otorga permiso para eliminar la ejecución de un flujo de trabajo	Escritura	run*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRunCache	Otorga permiso para eliminar la caché de ejecución de un flujo de trabajo	Escritura	runCache*		
DeleteRunGroup	Otorga permiso para eliminar un grupo de ejecuciones de flujos de trabajo	Escritura	runGroup*		
DeleteS3AccessPolicy	Otorga permiso para eliminar una política de acceso en una tienda determinada	Escritura	sequenceStore*		
DeleteSequenceStore	Otorga permiso para eliminar un almacén de secuencias	Escritura	sequenceStore*		
DeleteShare	Otorga permiso para eliminar un recurso compartido	Escritura			
DeleteVariantStore	Otorga permiso para eliminar un almacén de variantes	Escritura	VariantStore*		
DeleteWorkflow	Concede permiso para eliminar un flujo de trabajo	Escritura	workflow*		
DeleteWorkflowVersion	Otorga permiso para eliminar una versión del flujo de trabajo	Escritura	WorkflowVersion*		
			workflow*		
GetAnnotationImportJob	Otorga permiso para obtener el estado de un trabajo de importación de anotaciones	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAnnotationStore	Otorga permiso para obtener información detallada sobre un almacén de anotaciones	Lectura	AnnotationStore*		
GetAnnotationStoreVersion	Otorga permiso para obtener información detallada sobre una versión en un almacén de anotaciones	Lectura	AnnotationStoreVersion*		
GetReadSet	Otorga permiso para obtener un conjunto de lectura en el almacén de secuencias determinado	Lectura	readSet*		
			sequenceStore*		
GetReadSetActivationJob	Otorga permiso para obtener detalles sobre un trabajo de activación de conjuntos de lectura para el almacén de secuencias determinado	Lectura	sequenceStore*		
GetReadSetExportJob	Otorga permiso para obtener detalles sobre un trabajo de exportación de conjuntos de lectura para el almacén de secuencias determinado	Lectura	sequenceStore*		
GetReadSetImportJob	Otorga permiso para obtener detalles sobre un trabajo de importación de conjuntos de lectura para el almacén de secuencias determinado	Lectura	sequenceStore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetReadSetMetadata	Otorga permiso para obtener detalles sobre un conjunto de lectura en el almacén de secuencias determinado	Lectura	readSet*		
			sequenceStore*		
GetReference	Otorga permiso para obtener una referencia en el almacén de referencias determinado	Lectura	reference*		
			referenceStore*		
GetReferenceImportJob	Otorga permiso para obtener detalles sobre un trabajo de importación de referencias para el almacén de referencias determinado	Lectura	referenceStore*		
GetReferenceMetadata	Otorga permiso para obtener detalles sobre una referencia en el almacén de referencias determinado	Lectura	reference*		
			referenceStore*		
GetReferenceStore	Otorga permiso para obtener detalles sobre un almacén de referencias	Lectura	referenceStore*		
GetRun	Otorga permiso para recuperar los detalles de ejecución de un flujo de trabajo	Lectura	run*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRunCache	Otorga permiso para recuperar los detalles de la caché de ejecución del flujo de trabajo	Lectura	runCache*		
GetRunGroup	Otorga permiso para recuperar los detalles de un grupo de ejecuciones de flujos de trabajo	Lectura	runGroup*		
GetRunTask	Otorga permiso para recuperar los detalles de las tareas de un flujo de trabajo	Lectura	TaskResource* run*		
GetS3AccessPolicy	Otorga permiso para obtener detalles sobre una política de acceso en una tienda determinada	Lectura	sequenceStore*		
GetSequenceStore	Otorga permiso para obtener detalles sobre un almacén de secuencias	Lectura	sequenceStore*		
GetShare	Otorga permiso para obtener información detallada sobre un recurso compartido	Lectura			
GetVariantImportJob	Otorga permiso para obtener el estado de un trabajo de importación de variantes	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVariantStore	Otorga permiso para obtener información detallada sobre un almacén de variantes	Lectura	VariantStore*		
GetWorkflow	Otorga permiso para recuperar detalles de un flujo de trabajo	Lectura	workflow*		
GetWorkflowVersion	Otorga permiso para recuperar los detalles de la versión del flujo de trabajo	Lectura	WorkflowVersion*		
			workflow*		
ListAnnotationImportJobs	Otorga permiso para obtener una lista de trabajos de importación de anotaciones	Enumeración			
ListAnnotationStoreVersions	Otorga permiso para recuperar una lista de información sobre versiones en un almacén de anotaciones	Enumeración	AnnotationStore*		
ListAnnotationStores	Otorga permiso para recuperar una lista de información sobre los almacenes de anotaciones	Enumeración			
ListMultipartReadSetUploads	Concede permiso para enumerar cargas de conjuntos de lectura multiparte	Enumeración	sequenceStore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListReadSetActivationJobs	Otorga permiso para enumerar trabajos de activación de conjuntos de lectura para el almacén de secuencias determinado	Enumeración	sequenceStore*		
ListReadSetExportJobs	Otorga permiso para enumerar trabajos de exportación de conjuntos de lectura para el almacén de secuencias determinado	Enumeración	sequenceStore*		
ListReadSetImportJobs	Otorga permiso para enumerar trabajos de importación de conjuntos de lectura para el almacén de secuencias determinado	Enumeración	sequenceStore*		
ListReadSetUploadParts	Concede permiso para enumerar partes de cargas de conjuntos de lectura	Enumeración	sequenceStore*		
ListReadSets	Otorga permiso para enumerar conjuntos de lectura en el almacén de secuencias determinado	Enumeración	sequenceStore*		
ListReferenceImportJobs	Otorga permiso para enumerar trabajos de importación de referencias para el almacén de referencias determinado	Enumeración	referenceStore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListReferenceStores	Otorga permiso para enumerar los almacenes de referencias	Enumeración			
ListReferences	Otorga permiso para enumerar las referencias en el almacén de referencias determinado	Enumeración	referenceStore*		
ListRunCaches	Otorga permiso para recuperar una lista de cachés de ejecución de flujos de trabajo	Enumeración			
ListRunGroups	Otorga permiso para recuperar una lista de grupos de ejecuciones de flujos de trabajo	Enumeración			
ListRunTasks	Otorga permiso para recuperar una lista de tareas para la ejecución de un flujo de trabajo	Enumeración	run*		
ListRuns	Otorga permiso para recuperar una lista de ejecuciones de un flujo de trabajo	Enumeración			
ListSequenceStores	Otorga permiso para enumerar los almacenes de secuencias	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListShares	Otorga permiso para recuperar una lista de información sobre los recursos compartidos	Enumeración			
ListTagsForResource	Otorga permiso para recuperar una lista de etiquetas de recursos AWS	Enumeración			
ListVariantImportJobs	Otorga permiso para obtener una lista de trabajos de importación de variantes	Enumeración			
ListVariantStores	Otorga permiso para recuperar una lista de metadatos de los almacenes de variantes	Enumeración			
ListWorkflowVersions	Otorga permiso para recuperar una lista de versiones disponibles para un flujo de trabajo	Enumeración	workflow*		
ListWorkflows	Otorga permiso para recuperar una lista de flujos de trabajo disponibles	Enumeración			
PutS3AccessPolicy	Otorga permiso para poner una política de acceso en una tienda determinada	Escritura	sequenceStore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartAnnotationImportJob	Otorga permiso para importar una lista de archivos de anotación a un almacén de anotaciones	Escritura	AnnotationStore*		
			AnnotationStoreVersion*		
StartReadSetActivationJob	Otorga permiso para iniciar un trabajo de activación de conjuntos de lectura desde el almacén de secuencias determinado	Escritura	sequenceStore*		
StartReadSetExportJob	Otorga permiso para iniciar un trabajo de exportación de conjuntos de lectura desde el almacén de secuencias determinado	Escritura	sequenceStore*		
StartReadSetImportJob	Otorga permiso para iniciar un trabajo de importación de conjuntos de lectura en el almacén de secuencias determinado	Escritura	sequenceStore*		
StartReferenceImportJob	Otorga permiso para iniciar un trabajo de importación de referencias en el almacén de referencias determinado	Escritura	referenceStore*		
StartRun	Otorga permiso para iniciar la ejecución de un flujo de trabajo	Escritura	run*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			runCache		
			runGroup		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVariantImportJob	Otorga permiso para importar una lista de archivos de variantes a un almacén de variantes	Escritura	VariantStore*		
TagResource	Otorga permiso para añadir AWS etiquetas a un recurso	Etiquetado	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			readSet		
			reference		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar AWS etiquetas de recursos	Etiquetado	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			readSet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:TagKeys	
UpdateAnnotationStore	Otorga permiso para actualizar la información sobre el almacén de anotaciones	Escritura	AnnotationStore*		
UpdateAnnotationStoreVersion	Otorga permiso para actualizar la información sobre la versión en un almacén de anotaciones	Escritura	AnnotationStoreVersion*		
UpdateRunCache	Otorga permiso para actualizar la caché de ejecución de un flujo de trabajo	Escritura	runCache*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRunGroup	Otorga permiso para actualizar un grupo de ejecuciones de flujos de trabajo	Escritura	runGroup*		
UpdateSequenceStore	Otorga permiso para actualizar los detalles de un almacén de secuencias	Escritura	sequenceStore*		
UpdateVariantStore	Otorga permiso para actualizar los metadatos sobre el almacén de variantes	Escritura	VariantStore*		
UpdateWorkflow	Otorga permiso para actualizar los detalles del flujo de trabajo	Escritura	workflow*		
UpdateWorkflowVersion	Otorga permiso para actualizar los detalles de la versión del flujo de trabajo	Escritura	WorkflowVersion*		
			workflow*		
UploadReadSetPart	Concede permiso para cargar partes de conjuntos de lectura	Escritura	sequenceStore*		

Tipos de recursos definidos por AWS HealthOmics

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AnnotationStore	arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}	aws:ResourceTag/${TagKey}
AnnotationStoreVersion	arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}/version/${AnnotationStoreVersionName}	aws:ResourceTag/${TagKey}
readSet	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}/readSet/${ReadSetId}	aws:ResourceTag/${TagKey}
reference	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}/reference/${ReferenceId}	aws:ResourceTag/${TagKey}
referenceStore	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:omics:${Region}:${Account}:run/${Id}	aws:ResourceTag/${TagKey}
runCache	arn:${Partition}:omics:${Region}:${Account}:runCache/${Id}	aws:ResourceTag/${TagKey}
runGroup	arn:${Partition}:omics:${Region}:${Account}:runGroup/${Id}	aws:ResourceTag/${TagKey}
sequenceStore	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
TaggingResource	`arn:${Partition}:omics:${Region}:${Account}:tag/${TagKey}`	
TaskResource	`arn:${Partition}:omics:${Region}:${Account}:task/${Id}`	
VariantStore	`arn:${Partition}:omics:${Region}:${Account}:variantStore/${VariantStoreName}`	aws:ResourceTag/${TagKey}
workflow	`arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}`	aws:ResourceTag/${TagKey}
WorkflowVersion	`arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}/version/${VersionName}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS HealthOmics

AWS HealthOmics define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la presencia de los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Honeycode

Amazon Honeycode (prefijo de servicio: `honeycode`) proporciona las siguientes claves de contexto de recursos, acciones y claves de condición específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Honeycode
- Tipos de recursos definidos por Amazon Honeycode
- Claves de condición de Amazon Honeycode

Acciones definidas por Amazon Honeycode

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApproveTeamAssociation [solo permiso]	Otorga permiso para aprobar una solicitud de asociación de equipo para tu cuenta AWS	Escritura			
BatchCreateTableRows	Concede permiso para crear nuevas filas en una tabla	Write	table*		
BatchDeleteTableRows	Concede permiso para eliminar filas de una tabla	Write	table*		
BatchUpdateTableRows	Concede permiso para actualizar filas de una tabla	Write	table*		
BatchUpsertTableRows	Concede permiso para crear o actualizar filas en una tabla	Write	table*		
CreateTeam [solo permiso]	Concede permiso para crear un nuevo equipo de Amazon Honeycode para tu cuenta AWS	Escritura			
CreateTenant [solo permiso]	Otorga permiso para crear un nuevo inquilino en Amazon Honeycode para tu cuenta AWS	Escritura			
DeleteDomains [solo permiso]	Otorga permiso para eliminar los dominios de Amazon Honeycode de su cuenta AWS	Escritura			
DeregisterGroups [solo permiso]	Otorga permiso para eliminar grupos de un equipo de	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Amazon Honeycode para tu cuenta AWS				
DescribeTableDataImportJob	Concede permiso para obtener los detalles de un trabajo de importación de datos de tabla	Read	table*		
DescribeTeam [solo permiso]	Otorga permiso para obtener información sobre los equipos de Amazon Honeycode para su cuenta AWS	Lectura			
GetScreenData	Concede permiso para cargar los datos desde una pantalla	Read	screen*		
InvokeScreenAutomation	Concede permiso para invocar una automatización de pantalla	Write	screen-automation*		
ListDomains [solo permiso]	Otorga permiso para publicar todos los dominios de Amazon Honeycode y su estado de verificación en tu cuenta AWS	Enumeración			
ListGroups [solo permiso]	Otorga permiso para incluir en tu cuenta todos los grupos de un equipo de Amazon Honeycode AWS	Enumeración			
ListTableColumns	Concede permiso para enumerar las columnas de una tabla	List	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTableRows	Concede permiso para enumerar las filas de una tabla	List	table*		
ListTables	Concede permiso para enumerar las tablas de un libro	Enumeración	workbook*		
ListTagsForResource	Concede permiso para enumerar todas las etiquetas de un recurso	Etiquetado			
ListTeamAssociations [solo permiso]	Otorga permiso para incluir en su AWS cuenta todas las asociaciones de equipos pendientes y aprobadas	Enumeración			
ListTenants [solo permiso]	Otorga permiso para incluir en tu cuenta a todos los inquilinos de Amazon Honeycode AWS	Enumeración			
QueryTableRows	Concede permiso para consultar las filas de una tabla con un filtro	Read	table*		
RegisterDomainForVerification [solo permiso]	Concede permiso para solicitar la verificación de los dominios de Amazon Honeycode de su cuenta AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterGroups [solo permiso]	Otorga permiso para añadir grupos a un equipo de Amazon Honeycode para tu cuenta AWS	Escritura			
RejectTeamAssociation [solo permiso]	Otorga permiso para rechazar una solicitud de asociación de equipos para su cuenta AWS	Escritura			
RestartDomainVerification [solo permiso]	Concede permiso para reiniciar la verificación de los dominios de Amazon Honeycode de su cuenta AWS	Escritura			
StartTableDataImportJob	Concede permiso para iniciar un trabajo de importación de datos de tabla	Escritura	table*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado			
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado			
UpdateTeam [solo permiso]	Concede permiso para actualizar un equipo de Amazon Honeycode para tu cuenta AWS	Escritura			

Tipos de recursos definidos por Amazon Honeycode

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
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}`	

Claves de condición de Amazon Honeycode

Honeycode no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS IAM Access Analyzer

AWS El analizador de acceso de IAM (prefijo de servicio:`access-analyzer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IAM Access Analyzer
- Tipos de recursos definidos por AWS IAM Access Analyzer
- Claves de condición para AWS IAM Access Analyzer

Acciones definidas por AWS IAM Access Analyzer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApplyArchiveRule	Otorga permiso para aplicar una regla de archivo.	Write	Analyzer*		
CancelPolicyGeneration	Concede permiso para cancelar una generación de políticas	Escritura			
CheckAccessNotGranted	Concede permiso para comprobar que una política no	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	permite un acceso especificado				
CheckNoNewAccess	Concede permiso para comprobar que no se permite ningún acceso nuevo en comparación con una política existente	Lectura			
CheckNoPublicAccess	Concede permiso para confirmar que una política de recursos no permite el acceso público	Lectura			
CreateAccessPreview	Conceda permiso para crear una vista previa de acceso para el analizador especificado	Write	Analyzer*		
CreateAnalyzer	Otorga permiso para crear un analizador.	Write	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	Otorga permiso para crear una regla de archivo para el analizador especificado.	Write	ArchiveRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAnalyzer	Otorga permiso para eliminar el analizador especificado.	Write	Analyzer*		
DeleteArchiveRule	Otorga permiso para eliminar las reglas de archivo del analizador especificado.	Escritura	ArchiveRule*		
GenerateFindingRecommendation	Concede permiso para generar pasos de recomendación para resolver un hallazgo	Escritura	Analyzer*		
GetAccessPreview	Otorga permiso para obtener información acerca de una vista previa de acceso.	Read	Analyzer*		
GetAnalyzedResource	Otorga permiso para obtener información de un recurso analizado.	Read	Analyzer*		
GetAnalyzer	Otorga permiso para obtener información acerca de los analizadores.	Read	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	Otorga permiso para recuperar información acerca de las reglas de archivo del analizador especificado.	Read	ArchiveRule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFinding	Otorga permiso para obtener hallazgos.	Lectura	Analyzer*		
GetFindingRecommendation	Concede permiso para recuperar pasos de recomendación para resolver un hallazgo	Lectura	Analyzer*		
GetFindingsStatistics	Otorga permiso para recuperar estadísticas para los resultados	Lectura	Analyzer*		
GetGeneratedPolicy	Otorga permiso para recuperar una política que se generó mediante StartPolicyGeneration	Lectura			
ListAccessPreviewFindings	Otorga permiso para obtener una lista de hallazgos de una vista previa de acceso.	Read	Analyzer*		
ListAccessPreviews	Otorga permiso para recuperar una lista de vistas previas de accesos.	List	Analyzer*		
ListAnalyzedResources	Otorga permiso para obtener una lista de recursos analizados.	Read	Analyzer*		
ListAnalyzers	Otorga permiso para obtener una lista de analizadores.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListArchiveRules	Otorga permiso para obtener una lista de reglas de archivo de un analizador.	List	Analyzer*		
ListFindings	Otorga permiso para obtener una lista de hallazgos de un analizador.	Read	Analyzer*		
ListPolicyGenerations	Otorga permiso para mostrar todas las generaciones de políticas iniciadas recientemente	Read			
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas aplicadas a un recurso.	Read	Analyzer		
StartPolicyGeneration	Otorga permiso para iniciar una generación de políticas	Write			iam:PassRole
StartResourceScan	Otorga permiso para iniciar un análisis de las políticas aplicadas a un recurso.	Write	Analyzer*		
TagResource	Otorga permiso para agregar una etiqueta a un recurso.	Etiquetado	Analyzer		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	Analyzer		
				aws:TagKeys	
UpdateAnalyzer	Otorga permiso para modificar la configuración de un analizador	Escritura	Analyzer*		
UpdateArchiveRule	Otorga permiso para modificar una regla de archivo.	Write	ArchiveRule*		
UpdateFindings	Otorga permiso para modificar hallazgos.	Write	Analyzer*		
ValidatePolicy	Otorga permiso para validar una política	Read			

Tipos de recursos definidos por AWS IAM Access Analyzer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

Claves de condición para AWS IAM Access Analyzer

AWS IAM Access Analyzer define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Claves de acciones, recursos y condiciones del AWS IAM Identity Center

AWS El Centro de identidades de IAM (prefijo de servicio:`sso`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el Centro de Identidad de IAM AWS
- Tipos de recursos definidos por el Centro de Identidad de AWS IAM
- Claves de condición del centro de AWS identidad de IAM

Acciones definidas por el Centro de Identidad de IAM AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate Directory	Otorga permiso para conectar un directorio para que lo utilice el Centro de Identidad de AWS IAM	Escritura			ds:AuthorizeApplication
Associate Profile	Otorga permiso para crear una asociación entre un usuario o grupo del directorio y un perfil	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AttachCustomerManagedPolicyReferenceToPermissionSet	Concede permiso para adjuntar una referencia de política administrada por el cliente a un conjunto de permisos	Administración de permisos	Instance*		
			PermissionSet*		
AttachManagedPolicyToPermissionSet	Otorga permiso para adjuntar una política AWS gestionada a un conjunto de permisos	Administración de permisos	Instance*		
			PermissionSet*		
CreateAccountAssignment	Otorga permiso para asignar el acceso a un director a una persona específica Cuenta de AWS mediante un conjunto de permisos específico	Escritura	Account*		
			Instance*		
			PermissionSet*		
CreateApplication	Concede permiso para crear una aplicación.	Escritura	ApplicationProvider*		
			Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplicationAssignment	Concede permiso para crear una asignación de la aplicación	Escritura	Application*		
				sso:ApplicationAccount	
CreateApplicationInstance	Otorga permiso para añadir una instancia de aplicación al Centro de identidades de AWS IAM	Escritura			
CreateApplicationInstanceCertificate	Otorga permiso para agregar un certificado nuevo para una instancia de aplicación	Escritura			
CreateInstance	Concede permiso para crear una instancia de centro de identidad	Escritura	Instance*		iam:CreateServiceLinkedRole organizations:DescribeOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInstanceAccessControlAttributeConfiguration	Concede el permiso para habilitar la instancia para ABAC y especificar los atributos.	Escritura	Instance*		iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:UpdateAssumeRolePolicy
CreateManagedApplicationInstance	Otorga permiso para añadir una instancia de aplicación gestionada al Centro de identidades de AWS IAM	Escritura			
CreatePermissionSet	Otorga permiso para crear un conjunto de permisos	Write	Instance*		
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Otorga permiso para crear un perfil para una instancia de aplicación	Write			
CreateTrust	Otorga permiso para crear una confianza de federación en una cuenta de destino	Escritura			
CreateTrustedTokenIssuer	Concede permiso para crear un emisor de token de confianza para una instancia	Escritura	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	Otorga permiso para eliminar el acceso de un director de una instancia específica Cuenta de AWS mediante un conjunto de permisos específico	Escritura	Account*		
			Instance*		
			PermissionSet*		
DeleteApplication	Concede permiso para eliminar una aplicación.	Escritura	Application*		
				sso:ApplicationAccount	
DeleteApplicationAccessScope	Concede permiso para eliminar el ámbito del acceso a una aplicación	Escritura	Application*		
				sso:ApplicationAccount	
DeleteApplicationAssignment	Concede permiso para eliminar una asignación de la aplicación	Escritura	Application*		
				sso:ApplicationAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApplicationAuthenticationMethod	Concede permiso para eliminar un método de autenticación a una aplicación	Escritura	Application*		
				sso:ApplicationAccount	
DeleteApplicationGrant	Concede permiso para eliminar una concesión de una aplicación	Escritura	Application*		
				sso:ApplicationAccount	
DeleteApplicationInstance	Otorga permiso para eliminar la instancia de aplicación	Write			
DeleteApplicationInstanceCertificate	Otorga permiso para eliminar un certificado inactivo o caducado de la instancia de aplicación	Escritura			
DeleteInlinePolicyFromPermissionSet	Otorga permiso para eliminar la política en línea de un conjunto de permisos especificado	Escritura	Instance*		
			PermissionSet*		
DeleteInstance	Concede permiso para eliminar una instancia del centro de identidad	Escritura	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteInstanceAccessControlAttributeConfiguration	Concede el permiso para desactivar ABAC y quitar la lista de atributos para la instancia.	Write	Instance*		
DeleteManagedApplicationInstance	Otorga permiso para eliminar la instancia de aplicación administrada	Write			
DeletePermissionSet	Otorga permiso para eliminar un conjunto de permisos	Escritura	Instance* PermissionSet*		
DeletePermissionsBoundaryFromPermissionSet	Concede permiso para eliminar el límite de permisos de un conjunto de permisos	Administración de permisos	Instance* PermissionSet*		
DeletePermissionsPolicy	Otorga permiso para eliminar la política de permisos asociada a un conjunto de permisos	Permissions management			
DeleteProfile	Otorga permiso para eliminar el perfil de una instancia de aplicación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTrustedTokenIssuer	Concede permiso para eliminar un emisor de token de confianza para una instancia	Escritura	TrustedTokenIssuer*		
DescribeAccountAssignmentCreationStatus	Otorga permiso para describir el estado de la solicitud de creación de asignaciones	Lectura	Instance*		
DescribeAccountAssignmentDeletionStatus	Otorga permiso para describir el estado de una solicitud de eliminación de asignaciones	Lectura	Instance*		
DescribeApplication	Concede permiso para obtener información sobre una aplicación	Lectura	Application*		
				sso:ApplicationAccount	
DescribeApplicationAssignment	Concede permiso para recuperar una asignación de la aplicación	Lectura	Application*		
				sso:ApplicationAccount	
DescribeApplicationProvider	Concede el permiso para describir un proveedor de la aplicación	Lectura	ApplicationProvider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDirectories	Concede permiso para obtener información acerca de los directorios de esta cuenta	Lectura			
DescribeInstance	Concede permiso para obtener información acerca de una instancia del centro de identificación	Lectura	Instance*		
DescribeInstanceAccessControlAttributeConfiguration	Concede el permiso para obtener la lista de atributos utilizados por la instancia para ABAC.	Read	Instance*		
DescribePermissionSet	Otorga permiso para describir un conjunto de permisos	Lectura	Instance*		
			PermissionSet*		
DescribePermissionSetProvisioningStatus	Otorga permiso para describir el estado de la solicitud de aprovisionamiento de conjuntos de permisos	Lectura	Instance*		
DescribePermissionsPolicies	Otorga permiso para recuperar todas las política de permisos asociadas a un conjunto de permisos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRegisteredRegions	Otorga permiso para obtener las regiones en las que su organización ha habilitado el Centro de identidad de AWS IAM	Lectura			
DescribeTrustedTokenIssuer	Concede permiso para describir un emisor de token de confianza para una instancia	Lectura	TrustedTokenIssuer*		
DescribeTrusts	Concede permiso para obtener información acerca de las relaciones de confianza de esta cuenta	Lectura			
DetachCustomerManagedPolicyReferenceFromPermissionSet	Concede permiso para desasociar una referencia de política administrada por el cliente de un conjunto de permisos	Administración de permisos	Instance* PermissionSet*		
DetachManagedPolicyFromPermissionSet	Otorga permiso para separar la política AWS gestionada adjunta del conjunto de permisos especificado	Administración de permisos	Instance* PermissionSet*		
DisassociateDirectory	Otorga permiso para desasociar un directorio que vaya a ser utilizado por el Centro de Identidad de AWS IAM	Escritura			ds:UnauthorizeApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateProfile	Otorga permiso para desasociar a un usuario o grupo de directorio de un perfil	Escritura			
GetApplicationAccessScope	Concede permiso para obtener un ámbito de acceso a una aplicación	Lectura	Application*		
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	Concede permiso para leer configuraciones de asignación para una aplicación	Lectura	Application*		
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	Concede permiso para obtener un método de autenticación para una aplicación	Lectura	Application*		
				sso:ApplicationAccount	
GetApplicationGrant	Concede permiso para obtener detalles sobre una subvención que pertenece a una aplicación	Lectura	Application*		
				sso:ApplicationAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetApplicationInstance	Otorga permiso para recuperar detalles de una instancia de aplicación	Read			
GetApplicationTemplate	Otorga permiso para recuperar los detalles de la plantilla de aplicación	Lectura			
GetInlinePolicyForPermissionSet	Otorga permiso para obtener la directiva en línea asignada al conjunto de permisos	Lectura	Instance* PermissionSet*		
GetManagedApplicationInstance	Otorga permiso para recuperar detalles de una instancia de aplicación	Read			
GetMfaDeviceManagementForDirectory	Otorga permiso para recuperar la configuración de administración de dispositivos MFA para el directorio	Read			
GetPermissionSet	Otorga permiso para recuperar detalles de un conjunto de permisos	Lectura			
GetPermissionsBoundaryForPermissionSet	Concede permiso para obtener el límite de permisos de un conjunto de permisos	Lectura	Instance* PermissionSet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPermissionsPolicy	Otorga permiso para recuperar todos las políticas de permiso asociadas a un conjunto de permisos	Read			sso:DescribePermissionsPolicies
GetProfile	Otorga permiso para recuperar un perfil para una instancia de aplicación	Lectura			
GetSSOStatus	Otorga permiso para comprobar si el Centro de Identidad AWS de IAM está activado	Lectura			
GetSharedSsoConfiguration	Otorga permiso para recuperar la configuración compartida para la instancia de SSO actual	Read			
GetSsoConfiguration	Otorga permiso para recuperar la configuración de la instancia de SSO actual	Read			
GetTrust	Otorga permiso para recuperar la confianza de federación en una cuenta de destino	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportApplicationInstanceServiceProviderMetadata	Otorga permiso para actualizar la instancia de aplicación mediante la carga de una aplicación de archivos de metadatos de SAML proporcionado por el proveedor de servicios	Escritura			
ListAccountAssignmentCreationStatus	Otorga permiso para mostrar el estado de las solicitudes de creación de Cuenta de AWS asignaciones para una instancia de SSO específica	Enumeración	Instance*		
ListAccountAssignmentDeletionStatus	Otorga permiso para mostrar el estado de las solicitudes de eliminación de Cuenta de AWS asignaciones para una instancia de SSO específica	Enumeración	Instance*		
ListAccountAssignments	Otorga permiso para incluir en la lista al cesionario de lo especificado Cuenta de AWS con el conjunto de permisos especificado	Enumeración	Account*		
			Instance*		
			PermissionSet*		
ListAccountAssignmentsForPrincipal	Concede permiso para enumerar las cuentas asignadas a un usuario o grupo	Enumeración	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAccountsForProvisionedPermissionSet	Otorga permiso para enumerar todas las AWS cuentas en las que se aprovisiona el conjunto de permisos especificado	Enumeración	Instance*		
			PermissionSet*		
ListApplicationAccessScopes	Concede permiso para enumerar los ámbitos de acceso a una aplicación	Enumeración	Application*		
				sso:ApplicationAccount	
ListApplicationAssignments	Concede permiso para enumerar las asignaciones de la aplicación	Enumeración	Application*		
				sso:ApplicationAccount	
ListApplicationAssignmentsForPrincipal	Concede permiso para enumerar las aplicaciones asignadas a un usuario o grupo	Enumeración	Instance*		
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	Concede permiso para enumerar los métodos de autenticación a una aplicación	Enumeración	Application*		
				sso:ApplicationAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApplicationGrants	Concede el permiso para enumerar las concesiones de una aplicación	Enumeración	Application*		
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	Otorga permiso para recuperar todos los certificados de una determinada instancia de aplicación	Read			
ListApplicationInstances	Otorga permiso para recuperar todas las instancias de aplicación	Enumeración			sso:GetApplicationInstance
ListApplicationProviders	Concede permiso para enumerar los proveedores de la aplicación	Enumeración	ApplicationProvider*		
ListApplicationTemplates	Otorga permiso para recuperar todas las plantillas de aplicación admitidas	Enumeración			sso:GetApplicationTemplate
ListApplications	Concede permiso para recuperar todas las aplicaciones asociadas a la instancia de IAM Identity Center	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCustomerManagedPolicyReferencesInPermissionSet	Otorga permiso para enumerar las referencias de políticas administradas por el cliente adjuntas un conjunto de permisos	Enumeración	Instance* PermissionSet*		
ListDirectoryAssociations	Otorga permiso para recuperar detalles sobre el directorio conectado al Centro de Identidad de AWS IAM	Lectura			
ListInstances	Otorga permiso para enumerar las instancias de SSO a las que el autor de la llamada tiene acceso	Enumeración			
ListManagedPoliciesInPermissionSet	Otorga permiso para enumerar las políticas AWS administradas que se adjuntan a un conjunto de permisos específico	Enumeración	Instance* PermissionSet*		
ListPermissionSetProvisioningStatus	Otorga permiso para mostrar el estado de las solicitudes de aprovisionamiento de conjuntos de permisos para una instancia de SSO especificada	Enumeración	Instance*		
ListPermissionSets	Otorga permiso para recuperar todos los conjuntos de permisos	Enumeración	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPermissionSetsProvisionedToAccount	Otorga permiso para enumerar todos los conjuntos de permisos que se aprovisionan a un determinado Cuenta de AWS	Enumeración	Account*		
			Instance*		
ListProfileAssociations	Otorga permiso para recuperar el usuario o grupo de directorio asociado con el perfil	Read			
ListProfiles	Otorga permiso para recuperar todos los perfiles de una instancia de aplicación	Enumeración			sso:GetProfile
ListTagsForResource	Otorga permiso para obtener una lista de las etiquetas que se asocian a un recurso especificado	Lectura	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
ListTrustedTokenIssuers	Concede permiso para enumerar emisores de tokens de confianza para una instancia	Enumeración	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ProvisionPermissionSet	Concede permiso para aprovisionar un conjunto de permisos especificado en el destino especificado	Escritura	Account*		
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	Otorga permiso a create/update un ámbito de acceso a una aplicación	Escritura	Application*		
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	Concede permiso para agregar configuraciones de asignación a una aplicación	Escritura	Application*		
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	Concede permiso a create/update una aplicación para utilizar un método de autenticación	Escritura	Application*		
				sso:ApplicationAccount	
PutApplicationGrant	Concede permiso para conceder create/update una autorización a una aplicación	Escritura	Application*		
				sso:ApplicationAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutInlinePolicyToPermissionSet	Otorga permiso para adjuntar una directiva en línea de IAM a un conjunto de permisos	Escritura	Instance*		
			PermissionSet*		
PutMfaDeviceManagementForDirectory	Otorga permiso para poner la configuración de administración de dispositivos MFA para el directorio	Escritura			
PutPermissionsBoundaryToPermissionSet	Concede permiso para agregar el límite de permisos a un conjunto de permisos	Administración de permisos	Instance*		
			PermissionSet*		
PutPermissionsPolicy	Otorga permiso para agregar una directiva a un conjunto de permisos	Permissions management			
SearchGroups	Otorga permiso para buscar grupos dentro del directorio asociado	Read			ds:DescribeDirectories
SearchUsers	Otorga permiso para buscar usuarios dentro del directorio asociado	Lectura			ds:DescribeDirectories

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartSSO	Otorga permiso para inicializar el Centro de AWS Identidad de IAM	Escritura			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	Otorga permiso para asociar un conjunto de etiquetas a un recurso especificado	Etiquetado	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para desasociar un conjunto de etiquetas de un recurso especificado	Etiquetado	Application		
			Instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	Application*		
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	Otorga permiso para establecer un certificado como el activo para esta instancia de aplicación	Write			
UpdateApplicationInstanceDisplayData	Otorga permiso para actualizar los datos de visualización de una instancia de aplicación	Write			
UpdateApplicationInstanceResponseConfiguration	Otorga permiso para actualizar la configuración de respuesta de federación para la instancia de aplicación	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApplicationInstanceResponseSchemaConfiguration	Otorga permiso para actualizar la configuración de respuesta de esquema de federación para la instancia de aplicación	Write			
UpdateApplicationInstanceSecurityConfiguration	Otorga permiso para actualizar los detalles de seguridad para la instancia de aplicación	Write			
UpdateApplicationInstanceServiceProviderConfiguration	Otorga permiso para actualizar la configuración relacionada con el proveedor de servicios para la instancia de aplicación	Write			
UpdateApplicationInstanceStatus	Otorga permiso para actualizar el estado de una instancia de aplicación	Write			
UpdateDirectoryAssociation	Otorga permiso para actualizar los mapeos de atributos de usuario de tu directorio conectado	Escritura			
UpdateInstance	Concede permiso para actualizar una instancia del centro de identidad	Escritura	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateInstanceAccessControlAttributeConfiguration	Concede el permiso para actualizar los atributos que se utilizarán con la instancia de ABAC.	Write	Instance*		
UpdateManagedApplicationInstanceStatus	Otorga permiso para actualizar el estado de una instancia de aplicación administrada	Escritura			
UpdatePermissionSet	Otorga permiso para actualizar el conjunto de permisos	Administración de permisos	Instance* PermissionSet*		
UpdateProfile	Otorga permiso para actualizar el perfil de una instancia de aplicación	Write			
UpdateSSOConfiguration	Otorga permiso para actualizar la configuración de la instancia de SSO actual	Write			
UpdateTrust	Otorga permiso para actualizar la confianza de federación en una cuenta de destino	Escritura			
UpdateTrustedTokenIssuer	Concede permiso para actualizar un emisor de token de confianza para una instancia	Escritura	TrustedTokenIssuer*		

Tipos de recursos definidos por el Centro de Identidad de AWS IAM

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	aws:ResourceTag/${TagKey}
Account	`arn:${Partition}:sso:::account/${AccountId}`	
Instance	`arn:${Partition}:sso:::instance/${InstanceId}`	aws:ResourceTag/${TagKey}
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	aws:ResourceTag/${TagKey} sso:ApplicationAccount
TrustedTokenIssuer	`arn:${Partition}:sso::${AccountId}:trustedTokenIssuer/${InstanceId}/${TrustedTokenIssuerId}`	aws:ResourceTag/${TagKey}
ApplicationProvider	`arn:${Partition}:sso::aws:applicationProvider/${ApplicationProviderId}`	

Claves de condición del centro de AWS identidad de IAM

AWS El Centro de Identidad de IAM define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
sso:ApplicationAccount	Filtra el acceso por la cuenta que crea la aplicación. Esta clave de condición no es compatible con las aplicaciones SAML administradas por el cliente	Cadena

Claves de condición, recursos y acciones para el directorio del Centro de Identidad de AWS IAM

AWS El directorio del Centro de Identidad de IAM (prefijo de servicio:`sso-directory`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el directorio del Centro de Identidad de IAM AWS
- Tipos de recursos definidos por el directorio del Centro de Identidad de AWS IAM
- Claves de condición del directorio del Centro AWS de Identidad de IAM

Acciones definidas por el directorio del Centro de Identidad de IAM AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddMemberToGroup	Otorga permiso para añadir un miembro a un grupo en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
CompleteVirtualMfaDeviceRegistration	Otorga permiso para completar el proceso de creación de un dispositivo MFA virtual	Escritura			
CompleteWebAuthnDeviceRegistration	Otorga permiso para completar el proceso de registro de un dispositivo WebAuthn	Escritura			
CreateAlias	Otorga permiso para crear un alias para el directorio que el Centro de Identidad de AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	IAM proporciona de forma predeterminada				
CreateBearerToken	Otorga permiso para crear un token al portador para un inquilino de aprovisionamiento determinado	Write			
CreateExternalIdPConfigurationForDirectory	Otorga permiso para crear una configuración de proveedor de identidades externo para el directorio	Escritura			
CreateGroup	Otorga permiso para crear un grupo en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
CreateProvisioningTenant	Otorga permiso para crear un inquilino de aprovisionamiento para un directorio determinado	Escritura			
CreateUser	Otorga permiso para crear un usuario en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
DeleteBearerToken	Otorga permiso para eliminar un token de portador	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteExternalIdPCertificate	Otorga permiso para eliminar un certificado de IdP externo determinado	Write			
DeleteExternalIdPConfigurationForDirectory	Otorga permiso para eliminar una configuración de proveedor de identidades externo asociada al directorio	Escritura			
DeleteGroup	Otorga permiso para eliminar un grupo del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
DeleteMfaDeviceForUser	Otorga permiso para eliminar un dispositivo MFA por nombre de dispositivo de un usuario determinado	Write			
DeleteProvisioningTenant	Otorga permiso para eliminar el inquilino de aprovisionamiento	Escritura			
DeleteUser	Otorga permiso para eliminar un usuario del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDirectory	Otorga permiso para recuperar información sobre el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
DescribeGroup	Otorga permiso para consultar los datos del grupo, sin incluir usuarios ni miembros del grupo	Lectura			
DescribeGroups	Otorga permiso para recuperar información sobre los grupos del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
DescribeProvisioningTenant	Otorga permiso para eliminar el arrendatario de aprovisionamiento	Lectura			
DescribeUser	Otorga permiso para recuperar información sobre un usuario del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeUserByUniqueAttribute	Otorga permiso para describir al usuario con un atributo único válido representado para el usuario	Lectura			
DescribeUsers	Otorga permiso para recuperar información sobre el usuario del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
DisableExternalIdPConfigurationForDirectory	Otorga permiso para desactivar la autenticación de usuarios finales con un proveedor de identidades externo	Escritura			
DisableUser	Otorga permiso para desactivar un usuario en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
EnableExternalIdPConfigurationForDirectory	Otorga permiso para habilitar la autenticación de usuarios finales con un proveedor de identidades externo	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableUser	Otorga permiso para activar el usuario en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
GetAWSSPConfigurationForDirectory	Otorga permiso para recuperar las configuraciones del proveedor de servicios del AWS IAM Identity Center para el directorio	Lectura			
GetGroupId	Otorga permiso para recuperar la información de identificación sobre el grupo del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
GetUserId	Otorga permiso para recuperar la información de identificación del usuario del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
GetUserPoolInfo	(Obsoleto) Otorga permiso para obtener información UserPool	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportExternalIdPCertificate	Otorga permiso para importar el certificado de IdP utilizado para verificar respuestas de IdP externas	Escritura			
IsMemberInGroup	Otorga permiso para comprobar si un miembro forma parte del grupo del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
IsMemberInGroups	Otorga permiso para comprobar si un miembro forma parte de varios grupos del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
ListBearerTokens	Otorga permiso para enumerar tokens portadores para un inquilino de aprovisionamiento dado	Read			
ListExternalIdPCertificates	Otorga permiso para enumerar los certificados de IdP externos de un directorio e IdP determinados	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExternalIdPConfigurationsForDirectory	Otorga permiso para mostrar todas las configuraciones del proveedor de identidad es externo creadas para el directorio	Lectura			
ListGroups	Otorga permiso para enumerar grupos del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
ListGroupsForMember	Otorga permiso para crear una lista de los grupos del miembro de destino	Lectura			
ListGroupsForUser	Otorga permiso para enumerar grupos a un usuario desde el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
ListMembersInGroup	Otorga permiso para recuperar todos los miembros que forman parte de un grupo en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMfaDevicesForUser	Otorga permiso para mostrar todos los dispositivos MFA activos y los metadatos de dispositivo MFA para un usuario	Read			
ListProvisioningTenants	Otorga permiso para mostrar inquilinos de aprovisionamiento para un directorio determinado	Lectura			
ListUsers	Otorga permiso para incluir usuarios en una lista del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Lectura			
RemoveMemberFromGroup	Otorga permiso para eliminar a un miembro que forma parte de un grupo del directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
SearchGroups	Otorga permiso para buscar grupos dentro del directorio asociado	Read			
SearchUsers	Otorga permiso para buscar usuarios dentro del directorio asociado	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartVirtualMfaDeviceRegistration	Otorga permiso para iniciar el proceso de creación del dispositivo mfa virtual	Escritura			
StartWebAuthnDeviceRegistration	Otorga permiso para iniciar el proceso de registro de un dispositivo WebAuthn	Escritura			
UpdateExternalIdPConfigurationForDirectory	Otorga permiso para actualizar una configuración de proveedor de identidades externo asociada al directorio	Escritura			
UpdateGroup	Otorga permiso para actualizar la información sobre un grupo en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
UpdateGroupDisplayName	Otorga permiso para actualizar el nombre de visualización y la respuesta del nombre de visualización	Write			
UpdateMfaDeviceForUser	Otorga permiso para actualizar la información del dispositivo MFA.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePassword	Concede permiso para actualizar una contraseña enviando un enlace de restablecimiento de la contraseña por correo electrónico o generando una contraseña de un solo uso para un usuario en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
UpdateUser	Otorga permiso para actualizar la información del usuario en el directorio que el Centro de Identidad de AWS IAM proporciona de forma predeterminada	Escritura			
UpdateUserName	Otorga permiso para actualizar el nombre de usuario y la respuesta del nombre de usuario	Write			
VerifyEmail	Otorga permiso para comprobar una dirección de correo electrónico de un usuario	Escritura			

Tipos de recursos definidos por el directorio del Centro de Identidad de AWS IAM

AWS El directorio del centro de identidad de IAM no admite la especificación de un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso al directorio del centro de identidad de AWS IAM, `"Resource": "*"` especifíquelo en su política.

Claves de condición del directorio del Centro AWS de Identidad de IAM

El directorio del Centro de Identidad de IAM no tiene claves de contexto específicas de un servicio que puedan usarse como `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el servicio OIDC del Centro de Identidad de IAM de AWS

AWS El servicio OIDC de IAM Identity Center (prefijo de servicio:`sso-oauth`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio OIDC del Centro de Identificación de IAM de AWS
- Tipos de recursos definidos por el servicio OIDC del Centro de Identificación de IAM de AWS
- Claves de condición para el servicio OIDC del Centro de Identificación de IAM de AWS

Acciones definidas por el servicio OIDC del Centro de Identificación de IAM de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTokenWithIAM	Otorga permiso para crear OAuth/OIDC tokens para acceder a las aplicaciones integradas del IAM Identity Center	Escritura	Application*		

Tipos de recursos definidos por el servicio OIDC del Centro de Identificación de IAM de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	

Claves de condición para el servicio OIDC del Centro de Identificación de IAM de AWS

El servicio OIDC no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) (prefijo de servicio:`iam`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Identity and Access Management (IAM)
- Tipos de recursos definidos por AWS Identity and Access Management (IAM)
- Claves de condición para AWS Identity and Access Management (IAM)

Acciones definidas por AWS Identity and Access Management (IAM)

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddClientIDToOpenIDConnectProvider	Concede permiso para añadir un nuevo ID de cliente (audiencia) a la lista de registrados IDs para el recurso de proveedor de IAM OpenID Connect (OIDC) especificado	Escritura	oidc-provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddRoleToInstanceProfile	Concede permiso para agregar un rol de IAM al perfil de instancia especificado.	Write	instance-profile*		iam:PassRole
AddUserToGroup	Concede permiso para agregar un usuario de IAM en el grupo de IAM especificado.	Write	group*		
AttachGroupPolicy	Concede permiso para conectar una política administrada al grupo de IAM especificado.	Permissions management	group*		
				iam:PolicyARN	
AttachRolePolicy	Concede permiso para asociar una política administrada al rol de IAM especificado.	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
AttachUserPolicy	Concede permiso para conectar una política administrada al usuario de IAM especificado.	Administración de permisos	user*		
				iam:PolicyARN iam:PermissionsBoundary	
ChangePassword	Concede permiso a un usuario de IAM para que pueda cambiar su propia contraseña	Escritura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccessKey	Concede permiso para crear una clave de acceso y una clave de acceso secreta para el usuario de IAM especificado.	Escritura	user*		
CreateAccountAlias	Otorga permiso para crear un alias para su Cuenta de AWS	Escritura			
CreateGroup	Concede permiso para crear un nuevo grupo.	Write	group*		
CreateInstanceProfile	Concede permiso para crear un nuevo perfil de instancia.	Write	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoginProfile	Concede permiso para crear una contraseña para el usuario de IAM especificado.	Write	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateOpenIDConnectProvider	Concede permiso para crear un recurso de IAM que describe un proveedor de identidades (IdP) compatible con OpenID Connect (OIDC).	Write	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicy	Concede permiso para crear una política nueva administrada.	Permissions management	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicyVersion	Concede permiso para crear una nueva versión de la política administrada especificada.	Permissions management	policy*		
CreateRole	Concede permiso para crear un nuevo rol.	Write	role*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateSAMLProvider	Concede permiso para crear un recurso de IAM que describe un proveedor de identidades (IdP) compatible con SAML 2.0	Escritura	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceLinkedRole	Otorga permiso para crear un rol de IAM que permita a un AWS servicio realizar acciones en su nombre	Escritura	role*		
				iam:AWSServiceName	
CreateServiceSpecificCredential	Concede permiso para crear una nueva credencial específica del servicio para un usuario de IAM.	Write	user*		
CreateUser	Concede permiso para crear un nuevo usuario de IAM.	Write	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	Concede permiso para crear un nuevo dispositivo MFA virtual.	Write	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMFADevice	Concede permiso para desactivar el dispositivo MFA especificado y eliminar su asociación con el usuario de IAM para el que se habilitó originalmente.	Write	user*		
DeleteAccessKey	Concede permiso para eliminar el par de claves de acceso que está asociado con el usuario de IAM especificado.	Escritura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccountAlias	Otorga permiso para eliminar el alias especificado Cuenta de AWS	Escritura			
DeleteAccountPasswordPolicy	Otorga permiso para eliminar la política de contraseñas del Cuenta de AWS	Administración de permisos			
DeleteCloudFrontPublicKey	Otorga permiso para eliminar una clave CloudFront pública existente	Escritura			
DeleteGroup	Concede permiso para eliminar el grupo de IAM especificado.	Write	group*		
DeleteGroupPolicy	Concede permiso para eliminar la política insertada especificada de su grupo.	Permissions management	group*		
DeleteInstanceProfile	Concede permiso para eliminar el perfil de instancia especificado.	Write	instance-profile*		
DeleteLoginProfile	Concede permiso para eliminar la contraseña del usuario de IAM especificado.	Write	user*		
DeleteOpenIDConnectProvider	Concede permiso para eliminar un objeto de recurso de proveedor de identidades (IdP) OpenID Connect en IAM.	Write	oidc-provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePolicy	Concede permiso para borrar la política administrada especificada y eliminarla de todas las entidades de IAM (usuarios, grupos o roles) a las que está asociada.	Permissions management	policy*		
DeletePolicyVersion	Concede permiso para eliminar una versión de la política administrada especificada.	Permissions management	policy*		
DeleteRole	Concede permiso para eliminar el rol especificado.	Write	role*		
DeleteRolePermissionsBoundary	Concede permiso para eliminar los límites de permisos de un rol.	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteRolePolicy	Concede permiso para eliminar la política insertada especificada del rol especificado.	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteSAMLProvider	Concede permiso para eliminar un recurso de proveedor de SAML en IAM.	Write	saml-provider*		
DeleteSSHPublicKey	Concede permiso para eliminar la clave pública SSH especificada.	Write	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteServerCertificate	Concede permiso para eliminar el certificado de servidor especificado.	Escritura	server-certificate*		
DeleteServiceLinkedRole	Otorga permiso para eliminar un rol de IAM vinculado a un AWS servicio específico, si el servicio ya no lo usa	Escritura	role*		
DeleteServiceSpecificCredential	Concede permiso para eliminar una credencial específica del servicio para un usuario de IAM.	Write	user*		
DeleteSigningCertificate	Concede permiso para eliminar un certificado de firma que está asociado al usuario de IAM especificado.	Write	user*		
DeleteUser	Concede permiso para eliminar el usuario de IAM especificado.	Write	user*		
DeleteUserPermissionsBoundary	Concede permiso para eliminar los límites de permisos del usuario de IAM especificado.	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	Concede permiso para eliminar la política insertada especificada de un usuario de IAM.	Permissions management	user*		
				iam:PermissionsBoundary	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteVirtualMFADevice	Concede permiso para eliminar un dispositivo MFA virtual.	Write	mfa		
			sms-mfa		
DetachGroupPolicy	Concede permiso para desasociar una política administrada del grupo de IAM especificado.	Permissions management	group*		
				iam:PolicyARN	
DetachRolePolicy	Concede permiso para desasociar una política administrada del rol especificado.	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
DetachUserPolicy	Concede permiso para desasociar una política administrada del usuario de IAM especificado.	Administración de permisos	user*		
				iam:PolicyARN iam:PermissionsBoundary	
DisableOrganizationsRootCredentialsManagement	Otorga permiso para deshabilitar la administración de las credenciales de usuario raíz de una cuenta de miembro en una organización administrada con la cuenta corriente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableOrganizationsRootSessions	Otorga permiso para deshabilitar las acciones raíz privilegiadas en las cuentas de los miembros de una organización gestionada con la cuenta corriente	Escritura			
EnableMFADevice	Concede permiso para habilitar un dispositivo MFA y asociarla a la usuario de IAM especificado.	Escritura	user*		
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
EnableOrganizationsRootCredentialsManagement	Otorga permiso para habilitar la administración de las credenciales de usuario raíz de una cuenta de miembro de una organización administrada con la cuenta corriente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableOrganizationsRootSessions	Otorga permiso para habilitar acciones raíz privilegiadas en las cuentas de los miembros de una organización gestionada con la cuenta corriente	Escritura			
GenerateCredentialReport	Otorga permiso para generar un informe de credenciales para la Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateOrganizationsAccessReport	Otorga permiso para generar un informe de acceso para una entidad de AWS Organizations	Lectura	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy
				iam:OrganizationsPolicyId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateServiceLastAccessedDetails	Concede permiso para generar un informe de datos de los últimos servicios a los que se ha accedido para un recurso de IAM.	Read	group*		
			policy*		
			role*		
			user*		
GetAccessKeyLastUsed	Concede permiso para recuperar información acerca de cuándo se utilizó por última vez la clave de acceso especificada.	Lectura	user*		
GetAccountAuthorizationDetails	Otorga permiso para recuperar información sobre todos los usuarios, grupos, funciones y políticas de IAM que Cuenta de AWS tiene, incluidas sus relaciones entre sí	Lectura			
GetAccountEmailAddress	Concede permiso para recuperar la dirección de correo electrónico que está asociada a la cuenta	Lectura			
GetAccountName	Concede permiso para recuperar el nombre de cuenta que está asociado a la cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountPasswordPolicy	Otorga permiso para recuperar la política de contraseñas del Cuenta de AWS	Lectura			
GetAccountSummary	Otorga permiso para recuperar información sobre el uso de las entidades de IAM y las cuotas de IAM en el Cuenta de AWS	Enumeración			
GetCloudFrontPublicKey	Otorga permiso para recuperar información sobre la clave pública especificada CloudFront	Lectura			
GetContextKeysForCustomPolicy	Concede permiso para recuperar una lista de todas las claves de contexto a las que se hace referencia en la política especificada.	Read			
GetContextKeysForPrincipalPolicy	Concede permiso para recuperar una lista de todas las claves de contexto a los que se hace referencia en todas las políticas de IAM que se han asociado a la identidad de IAM especificada (usuario, grupo o rol).	Lectura	group		
			role		
			user		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCredentialReport	Otorga permiso para recuperar un informe de credenciales para Cuenta de AWS	Lectura			
GetGroup	Concede permiso para recuperar una lista de usuarios de IAM en el grupo de IAM especificado.	Read	group*		
GetGroupPolicy	Concede permiso para recuperar un documento de política insertada que está integrada en el grupo de IAM especificado.	Read	group*		
GetInstanceProfile	Concede permiso para recuperar información sobre el perfil de instancia especificado, incluidos la ruta del perfil de instancia, GUID, ARN y rol.	Read	instance-profile*		
GetLoginProfile	Concede permiso para recuperar la fecha de creación de la contraseña y el nombre de usuario del usuario de IAM especificado.	Enumeración	user*		
GetMFADevice	Concede permiso para recuperar información sobre un dispositivo MFA para el usuario especificado	Lectura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOpenIDConnectProvider	Concede permiso para recuperar información sobre el recurso de proveedor OpenID Connect (OIDC) especificado en IAM.	Lectura	oidc-provider*		
GetOrganizationsAccessReport	Otorga permiso para recuperar un informe de acceso de AWS Organizations	Lectura			
GetPolicy	Concede permiso para recuperar información sobre la política administrada especificada, incluida la versión predeterminada de la política y el número total de usuarios, grupos y roles de IAM a los que se asocia dicha política.	Read	policy*		
GetPolicyVersion	Concede permiso para recuperar información sobre una versión de la política administrada especificada, incluido el documento de política.	Read	policy*		
GetRole	Concede permiso para recuperar información sobre el rol especificado, incluidos la ruta del rol, GUID, ARN y la política de confianza del rol.	Read	role*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRolePolicy	Concede permiso para recuperar un documento de política insertada que está integrada con el rol de IAM especificado.	Read	role*		
GetSAMLProvider	Concede permiso para devolver el metadocumento del proveedor de SAML que se cargó cuando se cargó o actualizó el recurso de proveedor de SAML de IAM.	Read	saml-provider*		
GetSSHPublicKey	Concede permiso para recuperar la clave pública SSH especificada, incluidos los metadatos de la clave.	Read	user*		
GetServerCertificate	Concede permiso para recuperar información sobre el certificado de servidor especificado almacenado en IAM.	Read	server-certificate*		
GetServiceLastAccessedDetails	Concede permiso para recuperar información sobre el informe de datos de los últimos servicios a los que se ha accedido.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceLastAccessedDetailsWithEntities	Concede permiso para recuperar información sobre las entidades del informe de datos de los últimos servicios a los que se ha accedido.	Read			
GetServiceLinkedRoleDeletionStatus	Concede permiso para recuperar un estado de eliminación de rol vinculado a servicio de IAM.	Read	role*		
GetUser	En este ejemplo se muestra cómo recuperar información acerca del usuario de IAM especificado, incluidos la fecha de creación, la ruta, el ID exclusivo y el ARN del usuario.	Read	user*		
GetUserPolicy	Concede permiso para recuperar un documento de política insertada que está integrada en el usuario de IAM especificado.	Lectura	user*		
ListAccessKeys	Otorga permiso para mostrar información sobre la clave IDs de acceso asociada al usuario de IAM especificado	Enumeración	user*		
ListAccountAliases	Otorga permiso para incluir el alias de la cuenta asociado a Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAttachedGroupPolicies	Concede permiso para obtener una lista de todas las políticas administradas que se han asociado al grupo de IAM especificado.	List	group*		
ListAttachedRolePolicies	Concede permiso para obtener una lista de todas las políticas administradas que se asocian al rol de IAM especificado.	List	role*		
ListAttachedUserPolicies	Concede permiso para obtener una lista de todas las políticas administradas que se asocian al usuario de IAM especificado.	Enumeración	user*		
ListCloudFrontPublicKeys	Otorga permiso para enumerar todas las claves CloudFront públicas actuales de la cuenta	Enumeración			
ListEntitiesForPolicy	Concede permiso para obtener una lista de todas las identidades de IAM a la que se asocia la política administrada especificada.	List	policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGroupPolicies	Concede permiso para mostrar los nombres de las políticas insertadas que están integradas en el grupo de IAM especificado.	List	group*		
ListGroups	Concede permiso para obtener una lista de grupos de IAM con el prefijo de ruta especificado.	List			
ListGroupsForUser	Concede permiso para obtener una lista de grupos de IAM a los que pertenece el usuario de IAM especificado.	List	user*		
ListInstanceProfileTags	Concede permiso para obtener una lista de las etiquetas que se asocian al perfil de instancia especificado.	List	instance-profile*		
ListInstanceProfiles	Concede permiso para obtener una lista de los perfiles de instancia con el prefijo de ruta especificado.	List			
ListInstanceProfilesForRole	Concede permiso para obtener una lista de los perfiles de instancia que tienen el rol de IAM asociado especificado.	List	role*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMFADeviceTags	Concede permiso para obtener una lista de las etiquetas que se asocian al dispositivo MFA especificado.	List	mfa*		
ListMFADevices	Concede permiso para obtener una lista de los dispositivos MFA para un usuario de IAM.	List	user		
ListOpenIDConnectProviderTags	Concede permiso para enumerar las etiquetas que están adjuntas al proveedor OpenID Connect especificado	Enumeración	oidc-provider*		
ListOpenIDConnectProviders	Otorga permiso para mostrar información sobre los objetos de recursos del proveedor IAM OpenID Connect (OIDC) que se definen en el Cuenta de AWS	Enumeración			
ListOrganizationsFeatures	Otorga permiso para enumerar las funciones de acceso raíz centralizado habilitadas para su organización	Enumeración			
ListPolicies	Concede permiso para obtener una lista de todas las políticas administradas.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPoliciesGrantingServiceAccess	Concede permiso para mostrar información acerca de las políticas que conceden a una entidad acceso a un servicio específico.	List	group*		
			role*		
			user*		
ListPolicyTags	Concede permiso para obtener una lista de las etiquetas que se asocian a la política administrada especificada.	List	policy*		
ListPolicyVersions	Concede permiso para mostrar información acerca de las versiones de la política administrada especificada, incluida la versión que actualmente está establecida como la versión predeterminada de la política.	List	policy*		
ListRolePolicies	Concede permiso para mostrar los nombres de las políticas insertadas que están integradas en el rol de IAM especificado.	List	role*		
ListRoleTags	Concede permiso para obtener una lista de las etiquetas que se asocian al rol de IAM especificado.	List	role*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRoles	Concede permiso para obtener una lista de los roles de IAM con el prefijo de ruta especificado.	List			
ListSAMLProviderTags	Concede permiso para obtener una lista de las etiquetas que se asocian proveedor SAML especificado.	List	saml-provider*		
ListSAMLProviders	Concede permiso para obtener una lista de recursos del proveedor de SAML en IAM.	List			
ListSSHPublicKeys	Concede permiso para mostrar información acerca de las claves públicas SSH que están asociadas al usuario de IAM especificado.	Enumeración	user*		
ListSTSRegionalEndpointsStatus	Concede permiso para enumerar el estado de todos los puntos de conexión regionales de STS activos	Enumeración			
ListServerCertificateTags	Concede permiso para obtener una lista de las etiquetas que se asocian al certificado de servidor especificado.	List	server-certificate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServerCertificates	Concede permiso para obtener una lista de los certificados de servidor que tienen el prefijo de ruta especificado.	List			
ListServiceSpecificCredentials	Concede permiso para obtener una lista de credenciales específicas del servicio que están asociadas con el usuario de IAM especificado.	List	user*		
ListSigningCertificates	Concede permiso para mostrar información acerca de los certificados de firma que están asociadas al usuario de IAM especificado.	List	user*		
ListUserPolicies	Concede permiso para obtener una lista de los nombres de las políticas insertadas que están integradas en el usuario de IAM especificado.	List	user*		
ListUserTags	Concede permiso para obtener una lista de las etiquetas que se asocian al usuario de IAM especificado.	List	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListUsers	Concede permiso para obtener una lista de los usuarios de IAM con el prefijo de ruta especificado.	List			
ListVirtualMFADevices	Concede permiso para obtener una lista de dispositivos MFA virtuales por estado de asignación.	List			
PassRole [solo permiso]	Concede permiso para transferir un rol a un servicio.	Write	role*		
				iam:AssociatedResourceArn iam:PassedToService	
PutGroupPolicy	Concede permiso para crear o actualizar un documento de política insertada que está integrada en el grupo de IAM especificado.	Permissions management	group*		
PutRolePermissionsBoundary	Concede permiso para establecer una política administrada como un límite de permisos para un rol.	Permissions management	role*		
				iam:PermissionsBoundary	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutRolePolicy	Concede permiso para crear o actualizar un documento de política insertada que está integrada en el rol de IAM especificado.	Permissions management	role*		
				iam:PermissionsBoundary	
PutUserPermissionsBoundary	Concede permiso para establecer una política administrada como un límite de permisos para un usuario de IAM.	Permissions management	user*		
				iam:PermissionsBoundary	
PutUserPolicy	Concede permiso para crear o actualizar un documento de política insertada que está integrada en el usuario de IAM especificado.	Administración de permisos	user*		
				iam:PermissionsBoundary	
RemoveClientIDFromOpenIDConnectProvider	Concede permiso para eliminar el ID de cliente (audiencia) de la lista de clientes IDs en el recurso de proveedor de IAM OpenID Connect (OIDC) especificado	Escritura	oidc-provider*		
RemoveRoleFromInstanceProfile	Otorga permiso para eliminar un rol de IAM del perfil de instancia especificado EC2	Escritura	instance-profile*		
RemoveUserFromGroup	Concede permiso para eliminar un usuario de IAM del grupo especificado.	Write	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResetServiceSpecificCredential	Concede permiso para restablecer la contraseña de una credencial existente específica del servicio para un usuario de IAM.	Write	user*		
ResyncMFADevice	Concede permiso para sincronizar el dispositivo MFA especificado con su entidad de IAM (usuario o rol).	Write	user*		
SetDefaultPolicyVersion	Concede permiso para establecer la versión de la política especificada como la versión predeterminada de la política.	Administración de permisos	policy*		
SetSTSRegionalEndpointStatus	Concede permiso para activar o desactivar un punto de conexión regional de STS	Escritura			
SetSecurityTokenServicePreferences	Concede permiso para establecer la versión de token de punto de enlace global de STS.	Write			
SimulateCustomPolicy	Concede permiso para simular si una política basada en identidades o una política basada en recursos proporciona permisos para recursos y operaciones específicas de la API.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SimulatePrincipalPolicy	Concede permiso para simular si una política basada en identidades que está asociada a una entidad de IAM especificada (usuario o rol) proporciona permisos para recursos y operaciones específicas de la API.	Read	group		
			role		
			user		
TagInstanceProfile	Concede permiso para agregar etiquetas a un perfil de instancia	Etiquetado	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	Concede permiso para agregar etiquetas a un dispositivo MFA virtual	Etiquetado	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	Concede permiso para agregar etiquetas a un proveedor de OpenID Connect	Etiquetado	oidc-provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	Concede permiso para agregar etiquetas a una política administrada	Etiquetado	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagRole	Concede permiso para agregar etiquetas a un rol de IAM	Etiquetado	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagSAMLProvider	Concede permiso para agregar etiquetas a un proveedor SAML	Etiquetado	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagServerCertificate	Concede permiso para agregar etiquetas a un certificado de servidor	Etiquetado	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	Concede permiso para agregar etiquetas a un usuario de IAM	Etiquetado	user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	Concede permiso para eliminar las etiquetas especificadas del perfil de instancia	Etiquetado	instance-profile*		
				aws:TagKeys	
UntagMFADevice	Concede permiso para eliminar las etiquetas especificadas del dispositivo MFA virtual.	Etiquetado	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	Concede permiso para quitar las etiquetas especificadas del proveedor OpenID Connect	Etiquetado	oidc-provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UntagPolicy	Concede permiso para eliminar las etiquetas especificadas de la política administrada	Etiquetado	policy*		
				aws:TagKeys	
UntagRole	Concede permiso para eliminar las etiquetas especificadas del rol	Etiquetado	role*		
				aws:TagKeys	
UntagSAMLProvider	Concede permiso para eliminar las etiquetas especificadas del proveedor SAML	Etiquetado	saml-provider*		
				aws:TagKeys	
UntagServerCertificate	Concede permiso para eliminar las etiquetas especificadas del certificado de servidor	Etiquetado	server-certificate*		
				aws:TagKeys	
UntagUser	Concede permiso para eliminar las etiquetas especificadas del usuario	Etiquetado	user*		
				aws:TagKeys	
UpdateAccessKey	Concede permiso para actualizar el estado de la clave de acceso especificada como activo o inactivo.	Escritura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccountEmailAddress	Concede permiso para actualizar la dirección de correo electrónico que está asociada a la cuenta	Escritura			
UpdateAccountName	Concede permiso para actualizar el nombre de cuenta que está asociado a la cuenta	Escritura			
UpdateAccountPasswordPolicy	Otorga permiso para actualizar la configuración de la política de contraseñas del Cuenta de AWS	Escritura			
UpdateAssumeRolePolicy	Concede permiso para actualizar la política que concede permiso a una entidad de IAM para asumir un rol.	Administración de permisos	role*		
UpdateCloudFrontPublicKey	Otorga permiso para actualizar una clave CloudFront pública existente	Escritura			
UpdateGroup	Concede permiso para actualizar el nombre o la ruta del grupo de IAM especificado.	Write	group*		
UpdateLoginProfile	Concede permiso para cambiar la contraseña del usuario de IAM especificado.	Write	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateOpenIDConnectProviderThumbprint	Concede permiso para actualizar toda la lista de huellas digitales de certificado de servidor que están asociadas con un proveedor de proveedor OpenID Connect (OIDC).	Write	oidc-provider*		
UpdateRole	Concede permiso para actualizar la descripción o la configuración de duración máxima de la sesión de un rol.	Write	role*		
UpdateRoleDescription	Concede permiso para actualizar solo la descripción de un rol.	Write	role*		
UpdateSAMLProvider	Concede permiso para actualizar el documento de metadatos para un recurso de proveedor de SAML existente.	Write	saml-provider*		
UpdateSSHPublicKey	Concede permiso para actualizar el estado de la clave pública SSH del usuario de IAM como activa o inactiva.	Write	user*		
UpdateServerCertificate	Concede permiso para actualizar el nombre o la ruta del certificado de servidor especificado almacenado en IAM.	Write	server-certificate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceSpecificCredential	Concede permiso para actualizar el estado de una credencial específica del servicio como activa o inactiva para un usuario de IAM.	Write	user*		
UpdateSigningCertificate	Concede permiso para actualizar el estado del certificado de firma del usuario especificado como activo o inactivo.	Write	user*		
UpdateUser	Concede permiso para actualizar el nombre o la ruta del usuario de IAM especificado.	Escritura	user*		
UploadCloudFrontPublicKey	Otorga permiso para cargar una clave CloudFront pública	Escritura			
UploadSSHPublicKey	Concede permiso para cargar una clave pública SSH y asociarla al usuario de IAM especificado.	Escritura	user*		
UploadServerCertificate	Otorga permiso para cargar una entidad de certificado de servidor para Cuenta de AWS	Escritura	server-certificate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	Concede permiso para cargar un certificado de firma X.509 y asociarlo al usuario de IAM especificado.	Escritura	user*		

Tipos de recursos definidos por AWS Identity and Access Management (IAM)

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
access-report	`arn:${Partition}:iam::${Account}:access-report/${EntityPath}`	
assumed-role	`arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}`	

Tipos de recurso	ARN	Claves de condición
federated-user	arn:${Partition}:iam::${Account}:federated-user/${UserName}	
group	arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}	
instance-profile	arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}	aws:ResourceTag/${TagKey}
mfa	arn:${Partition}:iam::${Account}:mfa/${MfaTokenIdWithPath}	aws:ResourceTag/${TagKey}
oidc-provider	arn:${Partition}:iam::${Account}:oidc-provider/${OidcProviderName}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:iam::${Account}:policy/${PolicyNameWithPath}	aws:ResourceTag/${TagKey}
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
saml-provider	arn:${Partition}:iam::${Account}:saml-provider/${SamlProviderName}	aws:ResourceTag/${TagKey}
server-certificate	arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}	aws:ResourceTag/${TagKey}
sms-mfa	arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}	

Tipos de recurso	ARN	Claves de condición
user	`arn:${Partition}:iam::${Account}:user/${UserNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Claves de condición para AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString
iam:AWSServiceName	Filtra el acceso por AWS servicio al que está asociado este rol	Cadena
iam:AssociatedResourceArn	Filtra el acceso por el recurso en nombre del cual se usará el rol	ARN

Claves de condición	Descripción	Tipo
iam:FIDO-FIPS-140-2-certification	Filtra el acceso por el nivel de certificación de validación FIPS-140-2 del dispositivo MFA en el momento del registro de una clave de seguridad FIDO	Cadena
iam:FIDO-FIPS-140-3-certification	Filtra el acceso por el nivel de certificación de validación FIPS-140-3 del dispositivo MFA en el momento del registro de una clave de seguridad FIDO	Cadena
iam:FIDO-certification	Filtra el acceso por el nivel de certificación FIDO del dispositivo MFA en el momento del registro de una clave de seguridad FIDO	Cadena
iam:OrganizationsPolicyId	Filtra el acceso por el ID de la política de una AWS organización	Cadena
iam:PassedToService	Filtra el acceso por el AWS servicio al que se transfiere este rol	Cadena
iam:PermissionsBoundary	Filtra el acceso si la política especificada se establece como el límite de permisos en la entidad de IAM (usuario o rol).	ARN
iam:PolicyARN	Filtra el acceso por el ARN de una política de IAM.	ARN
iam:RegisterSecurityKey	Filtra el acceso según el estado actual de activación del dispositivo MFA	Cadena
iam:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a una entidad de IAM (usuario o rol).	Cadena

Acciones, recursos y claves de condición para AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere (prefijo de servicio:`rolesanywhere`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Identity and Access Management Roles Anywhere
- Tipos de recurso definidos por AWS Identity and Access Management Roles Anywhere
- Claves de condición para AWS Identity and Access Management Roles Anywhere

Acciones definidas por AWS Identity and Access Management Roles Anywhere

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla de acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProfile	Otorga permiso para crear un perfil.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTrustAnchor	Otorga permiso para crear un anclaje de confianza.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAttributeMapping	Concede permiso para eliminar una regla de asignación de un perfil	Escritura	profile*		
DeleteCrl	Otorga permiso para eliminar una lista de revocación de certificados (crl).	Escritura	crl*		
DeleteProfile	Concede permiso para eliminar un perfil	Escritura	profile*		
DeleteTrustAnchor	Otorga permiso para eliminar un anclaje de confianza.	Escritura	trust-anchor*		
DisableCrl	Otorga permiso para desactivar una lista de revocación de certificados (crl).	Escritura	crl*		
DisableProfile	Otorga permiso para desactivar un perfil.	Escritura	profile*		
DisableTrustAnchor	Otorga permiso para desactivar un anclaje de confianza.	Escritura	trust-anchor*		
EnableCrl	Otorga permiso para habilitar una lista de revocación de certificados (crl).	Escritura	crl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableProfile	Otorga permiso para habilitar un perfil.	Escritura	profile*		iam:PassRole
EnableTrustAnchor	Otorga permiso para habilitar un anclaje de confianza.	Escritura	trust-anchor*		
GetCrl	Otorga permiso para obtener una lista de revocación de certificados (crl).	Lectura	crl*		
GetProfile	Otorga permiso para obtener un perfil.	Lectura	profile*		
GetSubject	Otorga permiso para obtener un asunto.	Lectura	subject*		
GetTrustAnchor	Otorga permiso para obtener un anclaje de confianza.	Lectura	trust-anchor*		
ImportCrl	Otorga permiso para importar una lista de revocación de certificados (crl).	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	Otorga permiso para enumerar listas de revocación de certificados (crl).	Enumeración			
ListProfiles	Otorga permiso para enumerar perfiles.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSubjects	Otorga permiso para enumerar asuntos.	Enumeración			
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	Enumeración			
ListTrustAnchors	Otorga permiso para enumerar anclajes de confianza.	Enumeración			
PutAttributeMapping	Concede permiso para colocar una regla de asignación en un perfil	Escritura	profile*		
PutNotificationSettings	Concede permiso para asociar la configuración de notificaciones a un anclaje de confianza	Escritura	trust-anchor*		
ResetNotificationSettings	Concede permiso para restablecer la configuración de notificaciones personalizada al estado predeterminado definido por IAM Roles Anywhere	Escritura	trust-anchor*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	crl		
			profile		
			subject		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	
UpdateCrl	Otorga permiso para actualizar una lista de revocación de certificados (crl).	Escritura	crl*		
UpdateProfile	Otorga permiso para actualizar un perfil.	Escritura	profile*		iam:PassRole
UpdateTrustAnchor	Otorga permiso para actualizar un anclaje de confianza.	Escritura	trust-anchor*		

Tipos de recurso definidos por AWS Identity and Access Management Roles Anywhere

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
trust-anchor	`arn:${Partition}:rolesanywhere:${Region}:${Account}:trust-anchor/${TrustAnchorId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:rolesanywhere:${Region}:${Account}:profile/${ProfileId}`	aws:ResourceTag/${TagKey}
subject	`arn:${Partition}:rolesanywhere:${Region}:${Account}:subject/${SubjectId}`	aws:ResourceTag/${TagKey}
crl	`arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el almacén de identidades de AWS

AWS Identity Store (prefijo de servicio:`identitystore`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el almacén de identidades de AWS
- Tipos de recursos definidos por el almacén de identidades de AWS
- Claves de condición para el almacén de identidades de AWS

Acciones definidas por el almacén de identidades de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGroup	Otorga permiso para crear un grupo en el lugar especificado IdentityStore	Escritura	Identitystore*		
CreateGroupMembership	Otorga permiso para crear un miembro a un grupo del grupo especificado IdentityStore	Escritura	Group*		
			Identitystore*		
			User*		
CreateUser	Otorga permiso para crear un usuario en el especificado IdentityStore	Escritura	Identitystore*		
DeleteGroup	Otorga permiso para eliminar un grupo del grupo especificado IdentityStore	Escritura	Group*		
			Identitystore*		
DeleteGroupMembership	Otorga permiso para eliminar a un miembro que forma parte de un grupo del grupo especificado IdentityStore	Escritura	Group*		
			GroupMembership*		
			Identitystore*		
			User*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUser	Otorga permiso para eliminar un usuario del entorno especificado IdentityStore	Escritura	Identitystore*		
			User*		
DescribeGroup	Otorga permiso para recuperar información sobre un grupo del grupo especificado IdentityStore	Lectura	Group*		
			Identitystore*		
DescribeGroupMembership	Otorga permiso para recuperar información sobre un miembro que forma parte de un grupo del grupo especificado IdentityStore	Lectura	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DescribeUser	Otorga permiso para recuperar información sobre el usuario del especificado IdentityStore	Lectura	Identitystore*		
			User*		
GetGroupId	Otorga permiso para recuperar información de identificación sobre el grupo especificado IdentityStore	Lectura	Group*		
			Identitystore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGroupMembershipId	Otorga permiso para recuperar la información de identificación de un miembro que forma parte de un grupo del grupo especificado IdentityStore	Lectura	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
GetUserId	Otorga permiso para recuperar la información de identificación del usuario del usuario especificado IdentityStore	Lectura	Identitystore*		
			User*		
IsMemberInGroups	Otorga permiso para comprobar si un miembro forma parte de los grupos especificados IdentityStore	Lectura	AllGroupMemberships*		
			Group*		
			Identitystore*		
			User*		
ListGroupMemberships	Otorga permiso para recuperar todos los miembros que forman parte de un grupo del grupo especificado IdentityStore	Enumeración	AllGroupMemberships*		
			Group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Identitystore*		
ListGroupMembershipsForMember	Otorga permiso para enumerar los grupos del miembro de destino en el especificado IdentityStore	Enumeración	AllGroupMemberships*		
			Identitystore*		
			User*		
ListGroups	Otorga permiso para buscar grupos dentro del especificado IdentityStore	Enumeración	AllGroups*		
			Identitystore*		
ListUsers	Otorga permiso para buscar usuarios en el espacio especificado IdentityStore	Enumeración	AllUsers*		
			Identitystore*		
UpdateGroup	Otorga permiso para actualizar la información sobre un grupo del grupo especificado IdentityStore	Escritura	Group*		
			Identitystore*		
UpdateUser	Otorga permiso para actualizar la información del usuario en el espacio especificado IdentityStore	Escritura	Identitystore*		
			User*		

Tipos de recursos definidos por el almacén de identidades de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Identitystore	`arn:${Partition}:identitystore::${Account}:identitystore/${IdentityStoreId}`	
User	`arn:${Partition}:identitystore:::user/${UserId}`	
Group	`arn:${Partition}:identitystore:::group/${GroupId}`	
GroupMembership	`arn:${Partition}:identitystore:::membership/${MembershipId}`	
AllUsers	`arn:${Partition}:identitystore:::user/*`	
AllGroups	`arn:${Partition}:identitystore:::group/*`	
AllGroupMemberships	`arn:${Partition}:identitystore:::membership/*`	

Claves de condición para el almacén de identidades de AWS

AWS Identity Store define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las

que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
identitystore:UserId	Filtra el acceso por ID de usuario de IAM Identity Center	Cadena

Acciones, recursos y claves de condición para AWS Identity Store Auth

AWS Identity Store Auth (prefijo de servicio:`identitystore-auth`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Identity Store Auth
- Tipos de recursos definidos por AWS Identity Store Auth
- Claves de condición para AWS Identity Store Auth

Acciones definidas por AWS Identity Store Auth

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDeleteSession [solo permiso]	Concede permiso para eliminar un lote de sesiones especificadas	Escritura			
BatchGetSession [solo permiso]	Concede permiso para devolver los atributos de sesión de un lote de sesiones especificadas	Lectura			
ListSessions [solo permiso]	Concede permiso para recuperar una lista de sesiones activas para el usuario especificado	Enumeración			

Tipos de recursos definidos por AWS Identity Store Auth

AWS La autenticación del almacén de identidades no admite la especificación de un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso a AWS Identity Store Auth, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Identity Store Auth

Identity Store Auth no tiene claves de contexto específicas de servicios que se puedan usar en el elemento `Condition` de las instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Identity Synch

AWS Identity Sync (prefijo de servicio:`identity-sync`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Identity Sync
- Tipos de recurso definidos por AWS Identity Synch
- Claves de condición para AWS Identity Sync

Acciones definidas por AWS Identity Sync

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Concede permiso para configurar la entrega de registros suministrados para un perfil de sincronización	Administración de permisos	SyncProfileResource*		
CreateSyncFilter	Concede permiso para crear un filtro de sincronización en el perfil de sincronización	Escritura	SyncProfileResource*		
CreateSyncProfile	Concede permiso para crear un perfil de sincronización para el origen de identidad	Escritura			ds:AuthorizeApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSyncTarget	Concede permiso para crear un destino de sincronización para el origen de identidad	Escritura	SyncProfileResource*		
DeleteSyncFilter	Concede permiso para eliminar un filtro de sincronización del perfil de sincronización	Escritura	SyncProfileResource*		
DeleteSyncProfile	Concede permiso para eliminar un perfil de sincronización del origen	Escritura	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	Concede permiso para eliminar un destino de sincronización del origen	Escritura	SyncProfileResource*		
			SyncTargetResource*		
GetSyncProfile	Concede permiso para recuperar un perfil de sincronización al utilizar un nombre del perfil de sincronización	Lectura	SyncProfileResource*		
GetSyncTarget	Concede permiso para recuperar un destino de sincronización del perfil de sincronización	Lectura	SyncProfileResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			SyncTargetResource*		
ListSyncFilters	Concede permiso para enumerar los filtros de sincronización del perfil de sincronización	Enumeración	SyncProfileResource*		
StartSync	Concede permiso para iniciar un proceso de sincronización o para reanudar una sincronización que se detuvo previamente	Escritura	SyncProfileResource*		
StopSync	Concede permiso para detener el proceso de sincronización programada en el calendario de sincronización desde el inicio	Escritura	SyncProfileResource*		
UpdateSyncTarget	Concede permiso para actualizar un objetivo de sincronización en el perfil de sincronización	Escritura	SyncProfileResource*		
			SyncTargetResource*		

Tipos de recurso definidos por AWS Identity Synch

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
SyncProfileResource	`arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}`	
SyncTargetResource	`arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}`	

Claves de condición para AWS Identity Sync

Identity Sync no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Import Export Disk Service

AWS El servicio Import Export Disk (prefijo de servicio:`importexport`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Import Export Disk Service
- Tipos de recursos definidos por AWS Import Export Disk Service
- Claves de condición para AWS Import Export Disk Service

Acciones definidas por AWS Import Export Disk Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelJob	Esta acción cancela un trabajo especificado. Solo el propietario del trabajo puede cancelarlo. La acción produce un error si el trabajo ya ha comenzado o se ha completado.	Write			
CreateJob	Esta acción comienza el proceso de programar una carga o descarga de sus datos.	Escritura			
GetShippingLabel	Esta acción genera una etiqueta de envío prepagada que utilizarás para enviar el dispositivo AWS para su procesamiento.	Lectura			
GetStatus	Esta acción devuelve información sobre un trabajo, incluido dónde está el	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	trabajo en la canalización de procesamiento, el estado de los resultados y el valor de la firma asociado al trabajo.				
ListJobs	Esta acción devuelve los trabajos asociados con el solicitante.	List			
UpdateJob	La acción UpdateJob se utiliza para cambiar los parámetros que se haya especificado en el archivo de manifiesto original proporcionando un nuevo archivo de manifiesto.	Write			

Tipos de recursos definidos por AWS Import Export Disk Service

AWS El servicio Import Export Disk no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Import Export Disk Service, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Import Export Disk Service

Import/Export no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Inspector

Amazon Inspector (prefijo de servicio: `inspector`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Inspector
- Tipos de recurso definidos por Amazon Inspector
- Claves de condición de Amazon Inspector

Acciones definidas por Amazon Inspector

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddAttributesToFindings	Otorga permiso para asignar atributos (pares de claves y valores) a las conclusiones especificadas en ARNs las conclusiones	Escritura			
CreateAssessmentTarget	Otorga permiso para crear un nuevo objetivo de evaluación mediante el ARN del grupo	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de recursos generado por CreateResourceGroup				
CreateAssessmentTemplate	Otorga permiso para crear una plantilla de evaluación para el objetivo de evaluación que especifica el ARN del objetivo de evaluación	Write			
CreateExclusionsPreview	Otorga permiso para iniciar la generación de una vista previa de exclusiones para la plantilla de evaluación especificada	Escritura			
CreateResourceGroup	Otorga permiso para crear un grupo de recursos mediante el conjunto especificado de etiquetas (pares de claves y valores) que se utilizan para seleccionar las EC2 instancias que se incluirán en un objetivo de evaluación de Amazon Inspector	Escritura			
DeleteAssessmentRun	Otorga permiso para eliminar la ejecución de evaluación especificada por el ARN de la ejecución de evaluación	Write			
DeleteAssessmentTarget	Otorga permiso para eliminar el objetivo de evaluación especificado por el ARN del objetivo de evaluación	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAssessmentTemplate	Otorga permiso para eliminar la plantilla de evaluación que especifica el ARN de la plantilla de evaluación	Escritura			
DescribeAssessmentRuns	Otorga permiso para describir las ejecuciones de evaluación especificadas en cada una ARNs de las ejecuciones de evaluación	Lectura			
DescribeAssessmentTargets	Otorga permiso para describir los objetivos de la evaluación que se especifican en los objetivos ARNs de la evaluación	Lectura			
DescribeAssessmentTemplates	Otorga permiso para describir las plantillas de evaluación que se especifican en las plantillas ARNs de evaluación	Lectura			
DescribeCrossAccountAccessRole	Otorga permiso para describir la función de IAM que permite a Amazon Inspector acceder a su Cuenta de AWS	Lectura			
DescribeExclusions	Otorga permiso para describir las exclusiones especificadas en las exclusiones ARNs	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFindings	Otorga permiso para describir los hallazgos que se especifican en los ARNs hallazgos	Lectura			
DescribeResourceGroups	Otorga permiso para describir los grupos de recursos especificados por los grupos ARNs de recursos	Lectura			
DescribeRulesPackages	Otorga permiso para describir los paquetes de reglas que especifican los paquetes ARNs de reglas	Lectura			
GetAssessmentReport	Otorga permiso para producir un informe de evaluación que incluya resultados detallados y completos de una ejecución de evaluación especificada	Lectura			
GetExclusionsPreview	Otorga permiso para recuperar la vista previa de las exclusiones (una lista de ExclusionPreview objetos) especificada por el token de vista previa	Lectura			
GetTelemetryMetadata	Otorga permiso para obtener información sobre los datos que se recopilan para la ejecución de evaluación especificada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssessmentRunAgents	Otorga permiso para enumerar los agentes de las ejecuciones de evaluación que se especifican en las ejecuciones ARNs de evaluación	Enumeración			
ListAssessmentRuns	Otorga permiso para enumerar las series de evaluación que corresponden a las plantillas de evaluación especificadas en las plantillas ARNs de evaluación	Enumeración			
ListAssessmentTargets	Otorga permiso para enumerar los objetivos ARNs de la evaluación dentro de este Cuenta de AWS	Enumeración			
ListAssessmentTemplates	Otorga permiso para enumerar las plantillas de evaluación que corresponden a los objetivos de evaluación especificados en los objetivos ARNs de evaluación	Enumeración			
ListEventSubscriptions	Otorga permiso para enumerar todas las suscripciones a eventos de la plantilla de evaluación que especifica el ARN de la plantilla de evaluación	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListExclusions	Otorga permiso para enumerar exclusiones generadas por la ejecución de evaluación	Enumeración			
ListFindings	Otorga permiso para enumerar las conclusiones generadas por las series de evaluación y especificadas en las series ARNs de evaluación	Enumeración			
ListRulesPackages	Otorga permiso para enumerar todos los paquetes de reglas de Amazon Inspector disponibles	List			
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas asociadas a una plantilla de evaluación	Lectura			
PreviewAgents	Otorga permiso para previsualizar los agentes instalados en las EC2 instancias que forman parte del objetivo de evaluación especificado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterCrossAccountAccessRole	Otorga permiso para registrar la función de IAM que Amazon Inspector utiliza para enumerar sus EC2 instancias al inicio de la ejecución de la evaluación o cuando usted solicita la acción PreviewAgents	Escritura			
RemoveAttributesFromFindings	Otorga permiso para eliminar atributos completos (pares de clave y valor) de los resultados que se especifican en ARNs los hallazgos en los que existe un atributo con la clave especificada	Escritura			
SetTagsForResource	Otorga permiso para establecer etiquetas (pares de clave y valor) en la plantilla de evaluación que especifica el ARN de la plantilla de evaluación	Etiquetado			
StartAssessmentRun	Otorga permiso para iniciar la ejecución de evaluación especificada por el ARN de la plantilla de evaluación	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopAssessmentRun	Otorga permiso para detener la ejecución de evaluación especificada por el ARN de la ejecución de evaluación	Write			
SubscribeToEvent	Otorga permiso para habilitar el proceso de envío de notificaciones de Amazon Simple Notification Service (SNS) acerca de un evento especificado a un tema de SNS especificado	Write			
UnsubscribeFromEvent	Otorga permiso para desactivar el proceso de envío de notificaciones de Amazon Simple Notification Service (SNS) acerca de un evento especificado a un tema de SNS especificado.	Write			
UpdateAssessmentTarget	Otorga permiso para actualizar el objetivo de evaluación especificado por el ARN del objetivo de evaluación	Write			

Tipos de recurso definidos por Amazon Inspector

Amazon Inspector no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Amazon Inspector, especifique `"Resource": "*"` en su política.

Claves de condición de Amazon Inspector

Inspector no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Inspector2

Amazon Inspector2 (prefijo de servicio: `inspector2`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Inspector2
- Tipos de recursos definidos por Amazon Inspector2.
- Claves de condición de Amazon Inspector2

Acciones definidas por Amazon Inspector2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate Member	Otorga permiso para asociar una cuenta con una cuenta de administrador de Amazon Inspector.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetAccountStatus	Otorga permiso para recuperar información sobre las cuentas de Amazon Inspector para una cuenta.	Lectura			
BatchGetCodeSnippet	Concede permiso para recuperar información de fragmento de código sobre uno o varios resultados de vulnerabilidad de código	Lectura			
BatchGetFindingDetails	Concede permiso para permitir que un cliente obtenga información de vulnerabilidad mejorada de sus resultados	Lectura			
BatchGetFreeTrialInfo	Otorga permiso para recuperar la elegibilidad del periodo de prueba gratuito sobre las cuentas de Amazon Inspector para una cuenta.	Lectura			
BatchGetMemberEc2DeepInspectionStatus	Otorga permiso al administrador delegado para recuperar el estado de inspección profunda de ec2 de las cuentas de los miembros	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchUpdateMemberEc2DeepInspectionStatus	Otorga permiso para actualizar el estado de inspección profunda de ec2 por administrador delegado para sus cuentas de miembros asociadas	Escritura			
CancelFindingsReport	Concede permiso para cancelar la generación de un informe de resultados	Escritura			
CancelSbomExport	Concede permiso para cancelar la generación de un informe de SBOM	Escritura			
CreateCisScanConfiguration	Concede permiso para crear y definir la configuración de un análisis CIS	Escritura	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	Concede permiso para crear y definir la configuración de un filtro de resultados	Escritura	Filter*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	Otorga permiso para solicitar la generación de un informe de hallazgos.	Escritura			
CreateSbomExport	Concede permiso para solicitar la generación de un informe de SBOM	Escritura			
DeleteCisScanConfiguration	Concede permiso para eliminar una configuración de análisis CIS	Escritura	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
DeleteFilter	Otorga permiso para eliminar un filtro de hallazgos	Escritura	Filter*		
DescribeOrganizationConfiguration	Otorga permiso para recuperar información sobre los ajustes de configuración de Amazon Inspector de una AWS organización	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Disable	Otorga permiso para desactivar una cuenta de Amazon Inspector.	Escritura			
DisableDelegatedAdminAccount	Otorga permiso para deshabilitar una cuenta como cuenta de administrador delegado de Amazon Inspector para una organización AWS	Escritura			
DisassociateMember	Otorga permiso a una cuenta de administrador de Amazon Inspector para desasociarse de una cuenta de miembro de Inspector.	Escritura			
Enable	Otorga permiso para habilitar y especificar la configuración de una nueva cuenta de Amazon Inspector.	Escritura			
EnableDelegatedAdminAccount	Otorga permiso para habilitar una cuenta como cuenta de administrador delegado de Amazon Inspector para una organización AWS	Escritura			
GetCisScanReport	Concede permiso para recuperar un informe con información sobre análisis CIS completados	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCisScanResultDetails	Concede permiso para recuperar información sobre todos los detalles relacionados con un análisis CIS y un recurso objetivo	Enumeración			
GetClustersForImage	Otorga permiso para obtener la información del clúster de una imagen determinada de Amazon Ecr escaneada continuamente	Lectura			
GetConfiguration	Otorga permiso para recuperar información sobre los ajustes de configuración de Amazon Inspector para un Cuenta de AWS	Lectura			
GetDelegatedAdminAccount	Otorga permiso para recuperar información sobre la cuenta de administrador de Amazon Inspector para una cuenta.	Lectura			
GetEc2DeepInspectionConfiguration	Otorga permiso para recuperar la configuración de inspección profunda de ec2 para cuentas independientes, cuentas de administrador delegado y cuentas de miembro	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEncryptionKey	Concede permiso para recuperar información sobre la clave de KMS que se utiliza para cifrar fragmentos de código	Lectura			
GetFindingsReportStatus	Otorga permiso para recuperar el estado para un informe de hallazgos solicitado.	Lectura			
GetMember	Otorga permiso para recuperar información sobre una cuenta asociada a una cuenta de administrador de Amazon Inspector.	Lectura			
GetSbomExport	Concede permiso para recuperar un informe de SBOM solicitado	Lectura			
ListAccountPermissions	Otorga permiso para recuperar los permisos de configuración de características asociados a una cuenta de Amazon Inspector dentro de una organización.	Enumeración			
ListCisScanConfigurations	Concede permiso para recuperar información sobre todas las configuraciones de análisis CIS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCisScanResultsAggregatedByChecks	Concede permiso para recuperar información sobre todas las comprobaciones relacionadas con un análisis CIS	Enumeración			
ListCisScanResultsAggregatedByTargetResource	Concede permiso para recuperar información sobre todos los recursos relacionados con un análisis CIS	Enumeración			
ListCisScans	Concede permiso para recuperar información sobre análisis CIS completados	Enumeración			
ListCoverage	Otorga permiso para recuperar los tipos de estadísticas que Amazon Inspector puede generar para los recursos que Inspector monitorea.	Enumeración			
ListCoverageStatistics	Otorga permiso para recuperar datos estadísticos y otro tipo de información sobre los recursos que Amazon Inspector monitorea.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDelegatedAdminAccounts	Otorga permiso para recuperar información sobre la cuenta de administrador delegada de Amazon Inspector para una organización AWS	Enumeración			
ListFilters	Otorga permiso para recuperar información sobre todos los filtros de hallazgos	Enumeración			
ListFindingAggregations	Otorga permiso para recuperar datos estadísticos y otro tipo de información sobre los hallazgos de Amazon Inspector.	Enumeración			
ListFindings	Otorga permiso para recuperar un subconjunto de información sobre uno o más hallazgos	Enumeración			
ListMembers	Otorga permiso para recuperar información sobre las cuentas de miembro de Amazon Inspector asociadas a una cuenta de administrador de Inspector.	Enumeración			
ListTagsForResource	Otorga permiso para recuperar las etiquetas para un recurso de Amazon Inspector.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListUsageTotals	Otorga permiso para recuperar datos de uso agregados de una cuenta	Enumeración			
ResetEncryptionKey	Concede permiso para permitir que un cliente restablezca el uso de una clave de KMS propiedad de Amazon para cifrar fragmentos de código	Escritura			
SearchVulnerabilities	Concede permiso para enumerar detalles de cobertura de Amazon Inspector para una determinada vulnerabilidad	Lectura			
SendCisSessionHealth	Concede permiso para enviar el estado CIS para un análisis CIS	Escritura			
SendCisSessionTelemetry	Concede permiso para enviar telemetría CIS para un análisis CIS	Escritura			
StartCisSession	Concede permiso para iniciar una sesión de análisis CIS	Escritura			
StopCisSession	Concede permiso para detener una sesión de análisis CIS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar o actualizar las etiquetas para un recurso de Amazon Inspector.	Etiquetado	CIS Scan Configuration		
			Filter		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de Amazon Inspector.	Etiquetado	CIS Scan Configuration		
			Filter		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	Concede permiso para actualizar la configuración de un análisis CIS	Escritura	CIS Scan Configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	Otorga permiso para actualizar la información sobre los ajustes de configuración de Amazon Inspector para un Cuenta de AWS	Escritura			
UpdateEc2DeepInspectionConfiguration	Otorga permiso para actualizar la configuración de inspección profunda de ec2 mediante un administrador delegado, un miembro y una cuenta independiente	Escritura			
UpdateEncryptionKey	Concede permiso para que un cliente utilice una clave de KMS para cifrar fragmentos de código	Escritura			
UpdateFilter	Otorga permiso para actualizar la configuración de un filtro de hallazgos	Escritura	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateOrgEc2DeepInspectionConfiguration	Otorga permiso para actualizar la configuración de inspección profunda de ec2 mediante un administrador delegado para sus cuentas de miembros asociadas	Escritura			
UpdateOrganizationConfiguration	Otorga permiso para actualizar los ajustes de configuración de Amazon Inspector de una AWS organización	Escritura			

Tipos de recursos definidos por Amazon Inspector2.

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Filter	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/filter/${FilterId}`	aws:ResourceTag/${TagKey}
Finding	`arn:${Partition}:inspector2:${Region}:${Account}:finding/${FindingId}`	

Tipos de recurso	ARN	Claves de condición
CIS Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Inspector2

Amazon Inspector2 define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon InspectorScan

Amazon InspectorScan (prefijo de servicio:`inspector-scan`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon InspectorScan
- Tipos de recursos definidos por Amazon InspectorScan
- Claves de estado de Amazon InspectorScan

Acciones definidas por Amazon InspectorScan

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ScanSbom	Concede permiso para escanear la SBOM proporcionada por el cliente y devolver las vulnerabilidades detectadas en su interior	Lectura			

Tipos de recursos definidos por Amazon InspectorScan

Amazon InspectorScan no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a Amazon InspectorScan, `"Resource": "*"` especifícalo en tu política.

Claves de estado de Amazon InspectorScan

InspectorScan no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Interactive Video Service

Amazon Interactive Video Service (prefijo de servicio: `ivs`) proporciona los siguientes recursos específicos del servicio, acciones y claves de contexto de condición para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Interactive Video Service
- Tipos de recursos definidos por Amazon Interactive Video Service
- Claves de condición de Amazon Interactive Video Service

Acciones definidas por Amazon Interactive Video Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetChannel	Otorga permiso para obtener varios canales simultáneamente por el canal de ARN	Lectura	Channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetStreamKey	Otorga permiso para obtener varias claves de flujo simultáneamente mediante el ARN de clave de flujo	Lectura	Stream-Key*		
BatchStartViewerSessionRevocation	Otorga permiso para actuar StartViewerSessionRevocation en múltiples pares de ARN e ID de espectador de múltiples canales simultáneamente	Escritura	Channel*		
CreateChannel	Concede permiso para crear un canal nuevo y una clave de flujo asociado	Escritura	Channel*		
			Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEncoderConfiguration	Concede permiso para crear una nueva configuración del codificador	Escritura	Encoder-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIngestConfiguration	Concede permiso para crear una nueva configuración de ingesta	Escritura	Ingest-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateParticipantToken	Concede permiso para crear un token de participante	Escritura	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePlaybackRestrictionPolicy	Concede permiso para crear una política de restricción de reproducción	Escritura	Playback-Restriction-Policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRecordingConfiguration	Otorga permiso para crear una configuración de grabación nueva	Escritura	Recording-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStage	Concede permiso para crear una etapa	Escritura	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStorageConfiguration	Concede permiso para crear una nueva configuración del almacenamiento	Escritura	Storage-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamKey	Otorga permiso para crear una clave de flujo	Write	Stream-Key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Otorga permiso para eliminar un canal y las claves de flujo de un canal	Escritura	Channel*		
			Stream-Key*		
DeleteEncoderConfiguration	Concede permiso para eliminar una configuración de codificación para el ARN especificado	Escritura	Encoder-Configuration*		
DeleteIngestConfiguration	Concede permiso para eliminar una configuración de ingesta para el ARN especificado	Escritura	Ingest-Configuration*		
DeletePlaybackKeyPair	Otorga permiso para eliminar el par de claves de reproducción de un ARN especificado	Escritura	Playback-Key-Pair*		
DeletePlaybackRestrictionPolicy	Concede permiso para eliminar la política de restricción de reproducción para el ARN especificado	Escritura	Playback-Restriction-Policy*		
DeletePublicKey	Concede permiso para eliminar la clave pública para el ARN especificado	Escritura	Public-Key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRecordingConfiguration	Otorga permiso para eliminar una configuración de grabación para el ARN especificado	Escritura	Recording-Configuration*		
DeleteStage	Concede permiso para eliminar la etapa de un ARN especificado	Escritura	Stage*		
DeleteStorageConfiguration	Concede permiso para eliminar una configuración de almacenamiento para el ARN especificado	Escritura	Storage-Configuration*		
DeleteStreamKey	Otorga permiso para eliminar la clave de transmisión de un ARN especificado	Escritura	Stream-Key*		
DisconnectParticipant	Concede permiso para desconectar a un participante del ARN de etapa especificado	Escritura	Stage*		
GetChannel	Otorga permiso para obtener la configuración del canal para un canal especificado ARN	Lectura	Channel*		
GetComposition	Concede permiso a fin de obtener la composición para el ARN especificado	Lectura	Composition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEncoderConfiguration	Concede permiso para obtener la configuración del codificador para el ARN especificado	Lectura	Encoder-Configuration*		
GetIngestConfiguration	Concede permiso para obtener la configuración de ingesta para el ARN especificado	Lectura	Ingest-Configuration*		
GetParticipant	Concede permiso para obtener información de participante de un ARN de etapa, sesión y participante específicos	Lectura	Stage*		
GetPlaybackKeyPair	Otorga permiso para obtener la información del par de claves de reproducción de un ARN especificado	Lectura	Playback-Key-Pair*		
GetPlaybackRestrictionPolicy	Concede permiso para obtener la política de restricción de reproducción para el ARN especificado	Lectura	Playback-Restriction-Policy*		
GetPublicKey	Concede permiso para obtener la clave pública para el ARN especificado	Lectura	Public-Key*		
GetRecordingConfiguration	Otorga permiso para obtener la configuración de grabación para el ARN especificado	Lectura	Recording-Configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetStage	Concede permiso para obtener información de etapa de un ARN especificado	Lectura	Stage*		
GetStageSession	Concede permiso para obtener información de sesión de etapa de un ARN de etapa y una sesión especificados	Lectura	Stage*		
GetStorageConfiguration	Concede permiso para obtener la configuración de almacenamiento para el ARN especificado	Lectura	Storage-Configuration*		
GetStream	Otorga permiso para obtener información sobre la transmisión activa (en vivo) en un canal especificado	Read	Channel*		
GetStreamKey	Otorga permiso para obtener información de clave de transmisión para un ARN especificado	Lectura	Stream-Key*		
GetStreamSession	Otorga permiso para obtener información sobre la sesión de streaming en un canal especificado.	Lectura	Channel*		
ImportPlaybackKeyPair	Otorga permiso para importar la clave pública	Escritura	Playback-Key-Pair*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportPublicKey	Concede permiso para importar una clave pública	Escritura	Public-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListChannels	Otorga permiso para obtener información resumida sobre los canales	Enumeración	Channel*		
ListCompositions	Concede permiso para obtener información resumida sobre las composiciones	Enumeración	Encoder-Configuration		
			Stage		
ListEncoderConfigurations	Concede permiso para obtener información resumida sobre las configuraciones del codificador	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIngestConfigurations	Concede permiso para obtener información resumida sobre configuraciones de ingesta	Enumeración			
ListParticipantEvents	Concede permiso para enumerar los eventos de los participantes para un ARN de etapa, una sesión y un participante específicos	Enumeración	Stage*		
ListParticipantReplicas	Otorga permiso para obtener información resumida sobre las réplicas de los participantes	Enumeración	Stage*		
ListParticipants	Concede permiso para incluir a los participantes de un ARN de etapa y una sesión específicos	Enumeración	Stage*		
ListPlaybackKeyPairs	Otorga permiso para obtener información resumida sobre pares de claves de reproducción	Enumeración	Playback-Key-Pair*		
ListPlaybackRestrictionPolicies	Concede permiso para obtener información resumida sobre políticas de restricción de reproducción	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPublicKeys	Concede permiso para obtener información resumida sobre claves públicas	Enumeración			
ListRecordingConfigurations	Otorga permiso para obtener información de resumen sobre las configuraciones de grabación	Enumeración	Recording-Configuration*		
ListStageSessions	Concede permiso para enumerar las sesiones de etapa para un ARN de etapa específico	Enumeración	Stage*		
ListStages	Concede permiso para obtener información resumida sobre las etapas	Enumeración	Stage*		
ListStorageConfigurations	Concede permiso para obtener información resumida sobre las configuraciones del almacenamiento	Enumeración			
ListStreamKeys	Otorga permiso para obtener información resumida sobre las claves de transmisión	Enumeración	Channel*		
			Stream-Key*		
ListStreamSessions	Otorga permiso para obtener información resumida sobre la sesión de streaming en un canal especificado.	Enumeración	Channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStreams	Otorga permiso para obtener información resumida sobre transmisiones en directo	List	Channel*		
ListTagsForResource	Otorga permiso para obtener información sobre las etiquetas de un ARN especificado	Read	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutMetadata	Otorga permiso para insertar metadatos en una transmisión RTMP para un canal especificado	Escritura	Channel*		
StartComposition	Concede permiso para iniciar una nueva composición	Escritura	Encoder-Configuration*		
			Stage*		
			Channel		
			Storage-Configuration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
StartParticipantReplication	Otorga permiso para iniciar una réplica de un nuevo participante	Escritura	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
StartViewerSessionRevocation	Otorga permiso para iniciar el proceso de revocación de la sesión del espectador asociada con un ARN de canal e ID de espectador específicos	Escritura	Channel*		
StopComposition	Concede permiso para detener la composición para el ARN especificado	Escritura	Composition*		
StopParticipantReplication	Otorga permiso para detener la replicación del participante para el ARN especificado	Escritura	Stage*		
StopStream	Otorga permiso para desconectar a un transmisor en un canal especificado	Write	Channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar o actualizar etiquetas para un recurso con un ARN especificado	Etiquetado	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para quitar etiquetas de un recurso con un ARN especificado	Etiquetado	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys	
UpdateChannel	Otorga permiso para actualizar la configuración de un canal	Escritura	Channel*		
UpdateIngestConfiguration	Concede permiso para actualizar la configuración de ingesta para el ARN especificado	Escritura	Ingest-Configuration*		
UpdatePlaybackRestrictionPolicy	Concede permiso para actualizar la política de restricción de reproducción para el ARN especificado	Escritura	Playback-Restriction-Policy*		
UpdateStage	Concede permiso para actualizar la configuración de una etapa	Escritura	Stage*		

Tipos de recursos definidos por Amazon Interactive Video Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Channel	`arn:${Partition}:ivs:${Region}:${Account}:channel/${ResourceId}`	aws:ResourceTag/${TagKey}
Stream-Key	`arn:${Partition}:ivs:${Region}:${Account}:stream-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Key-Pair	`arn:${Partition}:ivs:${Region}:${Account}:playback-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Restriction-Policy	`arn:${Partition}:ivs:${Region}:${Account}:playback-restriction-policy/${ResourceId}`	aws:ResourceTag/${TagKey}
Recording-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:recording-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}
Stage	`arn:${Partition}:ivs:${Region}:${Account}:stage/${ResourceId}`	aws:ResourceTag/${TagKey}
Composition	`arn:${Partition}:ivs:${Region}:${Account}:composition/${ResourceId}`	aws:ResourceTag/${TagKey}
Encoder-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:encoder-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Storage-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:storage-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}
Public-Key	`arn:${Partition}:ivs:${Region}:${Account}:public-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Ingest-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:ingest-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Interactive Video Service

Amazon Interactive Video Service define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Interactive Video Service Chat

Amazon Interactive Video Service Chat (prefijo de servicio: `ivschat`) proporciona los siguientes recursos específicos del servicio, acciones y claves de contexto de condición para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Interactive Video Service Chat
- Tipos de recursos definidos por Amazon Interactive Video Service Chat
- Claves de condición de Amazon Interactive Video Service Chat

Acciones definidas por Amazon Interactive Video Service Chat

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateChatToken	Otorga permiso para crear un token cifrado que se utiliza para establecer una WebSocket conexión individual con una sala	Escritura	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLoggingConfiguration	Otorga permiso para crear una configuración de registro que permita a los clientes grabar mensajes de sala	Escritura	Logging-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoom	Concede permisos para crear una sala que permita a los clientes conectarse y pasar mensajes	Escritura	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLoggingConfiguration	Otorga permiso para eliminar la configuración de registro para un ARN de configuración de registro especificado	Escritura	Logging-Configuration*		
DeleteMessage	Otorga permiso para enviar un evento a una sala específica que indica a los clientes que eliminen un mensaje específico	Escritura	Room*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRoom	Otorga permiso para eliminar la sala para un ARN especificado de sala	Escritura	Room*		
DisconnectUser	Otorga permiso para desconectar todas las conexiones mediante una ID de usuario especificado de una sala	Escritura	Room*		
GetLoggingConfiguration	Otorga permiso para obtener la configuración de registro para un ARN de configuración de registro especificado	Lectura	Logging-Configuration*		
GetRoom	Otorga permiso para obtener la configuración de sala para un ARN especificado de sala	Lectura	Room*		
ListLoggingConfigurations	Otorga permiso para obtener información resumida sobre las configuraciones de registro	Enumeración	Logging-Configuration*		
ListRooms	Otorga permiso para obtener información resumida sobre las salas	Enumeración	Room*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para obtener información sobre las etiquetas de un ARN especificado	Lectura	Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
SendEvent	Otorga permisos para enviar un evento a una sala	Escritura	Room*		
TagResource	Otorga permiso para agregar o actualizar etiquetas para un recurso con un ARN especificado	Etiquetado	Logging-Configuration		
			Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para quitar etiquetas de un recurso con un ARN especificado	Etiquetado	Logging-Configuration		
			Room		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateLoggingConfiguration	Otorga permiso para actualizar la configuración de registro para un ARN de configuración de registro especificado	Escritura	Logging-Configuration*		
UpdateRoom	Otorga permiso para actualizar la configuración de una sala para el ARN especificado de sala	Escritura	Room*		

Tipos de recursos definidos por Amazon Interactive Video Service Chat

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Room	`arn:${Partition}:ivschat:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
Logging-Configuration	`arn:${Partition}:ivschat:${Region}:${Account}:logging-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Interactive Video Service Chat

Amazon Interactive Video Service Chat define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Invoicing Service

AWS El servicio de facturación (prefijo de servicio:`invoicing`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Invoicing Service
- Tipos de recursos definidos por AWS Invoicing Service
- Claves de condición para AWS Invoicing Service

Acciones definidas por AWS Invoicing Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetInvoiceProfile	Otorga permiso para obtener los detalles del perfil de facturación de una cuenta de su organización	Lectura			
CreateInvoiceUnit	Otorga permiso para crear una unidad de facturación para su organización	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteInvoiceUnit	Otorga permiso para actualizar una unidad de facturación para su organización	Escritura	invoice-unit*		
				aws:ResourceTag/${TagKey}	
GetInvoiceEmailDeliveryPreferences [solo permiso]	Concede permiso para obtener las preferencias de entrega de facturas por correo electrónico	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetInvoicePDF [solo permiso]	Concede permiso para obtener una factura en PDF	Lectura			
GetInvoiceUnit	Otorga permiso para obtener unidades de factura para su organización	Lectura	invoice-unit*		
ListInvoiceSummaries	Concede permiso para obtener información de resumen de factura para la cuenta o cuenta vinculada	Lectura			
ListInvoiceUnits	Otorga permiso para incluir las unidades de facturación de su organización	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	invoice-unit*		
				aws:ResourceTag/${TagKey}	
PutInvoiceEmailDeliveryPreferences [solo permiso]	Concede permiso para poner preferencias de entrega de facturas por correo electrónico	Escritura			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	invoice-unit*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	invoice-unit*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	Otorga permiso para actualizar una unidad de facturación para su organización	Escritura	invoice-unit*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS Invoicing Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
invoice-unit	`arn:${Partition}:invoicing::${Account}:invoice-unit/${Identifier}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Invoicing Service

AWS El servicio de facturación define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS IoT 1-Click

AWS IoT 1-Click (prefijo de servicio:`iot1click`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT 1-Click
- Tipos de recursos definidos por AWS IoT 1-Click
- Claves de condición para AWS IoT 1-Click

Acciones definidas por AWS IoT 1-Click

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateDeviceWithPlacement	Otorga permiso para asociar un dispositivo a una ubicación	Write	project*		
ClaimDevicesByClaimCode	Otorga permiso para reclamar un lote de dispositivos con un código de reclamación	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePlacement	Otorga permiso para crear una nueva ubicación en un proyecto	Write	project*		
CreateProject	Concede permiso para crear un nuevo proyecto	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlacement	Otorga permiso para eliminar una ubicación de un proyecto	Write	project*		
DeleteProject	Concede permiso para eliminar un proyecto	Write	project*		
DescribeDevice	Otorga permiso para describir un dispositivo	Read	device*		
DescribePlacement	Otorga permiso para describir una ubicación	Read	project*		
DescribeProject	Concede permiso para describir un proyecto	Read	project*		
DisassociateDeviceFromPlacement	Otorga permiso para desasociar un dispositivo de una ubicación	Write	project*		
FinalizeDeviceClaim		Read	device*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para finalizar la reclamación de un dispositivo			aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceMethods	Otorga permiso para obtener los métodos disponibles de un dispositivo	Read	device*		
GetDevicesInPlacement	Otorga permiso para obtener dispositivos asociados a una ubicación	Read	project*		
InitiateDeviceClaim	Otorga permiso para iniciar la reclamación de un dispositivo	Read	device*		
InvokeDeviceMethod	Otorga permiso para invocar un método de dispositivo	Write	device*		
ListDeviceEvents	Otorga permiso para enumerar eventos pasados publicados por un dispositivo	Read	device*		
ListDevices	Otorga permiso para enumerar todos los dispositivos	List			
ListPlacements	Otorga permiso para enumerar ubicaciones en un proyecto	Read	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProjects	Otorga permiso para enumerar todos los proyectos	List			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso.	Read	device		
			project		
TagResource	Otorga permisos para agregar o modificar las etiquetas de un recurso.	Etiquetado	device		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnclaimDevice	Otorga permiso para anular la reclamación de un dispositivo	Read	device*		
UntagResource	Otorga permiso para eliminar las etiquetas (metadatos) dadas de un recurso.	Etiquetado	device		
			project		
				aws:TagKeys	
UpdateDeviceState	Otorga permiso para actualizar el estado del dispositivo	Write	device*		
UpdatePlacement	Otorga permiso para actualizar una ubicación	Write	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateProject	Actualiza un proyecto.	Write	project*		

Tipos de recursos definidos por AWS IoT 1-Click

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
device	`arn:${Partition}:iot1click:${Region}:${Account}:devices/${DeviceId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:iot1click:${Region}:${Account}:projects/${ProjectName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT 1-Click

AWS IoT 1-Click define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso.	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS IoT Analytics

AWS IoT Analytics (prefijo de servicio:`iotanalytics`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Analytics
- Tipos de recursos definidos por AWS IoT Analytics
- Claves de condición para AWS IoT Analytics

Acciones definidas por AWS IoT Analytics

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchPutMessage	Pone un lote de mensajes en el canal especificado	Escritura	channel*		
CancelPipelineReprocessing	Cancela el reprocesado de la canalización especificada	Escritura	pipeline*		
CreateChannel	Crea un canal	Escritura	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Crea un conjunto de datos.	Escritura	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	Genera contenido del conjunto de datos especificado (ejecutando las acciones del conjunto)	Escritura	dataset*		
CreateDatastore	Crea un almacén de datos	Escritura	datastore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Crea una canalización	Escritura	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Elimina el canal especificado	Escritura	channel*		
DeleteDataset	Elimina el conjunto de datos especificado	Escritura	dataset*		
DeleteDatasetContent	Elimina el contenido del conjunto de datos especificado	Escritura	dataset*		
DeleteDatastore	Elimina el almacén de datos especificado	Escritura	datastore*		
DeletePipeline	Elimina la canalización especificada	Escritura	pipeline*		
DescribeChannel	Describe el canal especificado	Lectura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDataset	Describe el conjunto de datos especificado	Lectura	dataset*		
DescribeDatastore	Describe el almacén de datos especificado	Lectura	datastore*		
DescribeLoggingOptions	Describe las opciones de registro para la cuenta	Lectura			
DescribePipeline	Describe la canalización especificada	Lectura	pipeline*		
GetDatasetContent	Obtiene el contenido del conjunto de datos especificado	Lectura	dataset*		
ListChannels	Muestra una lista de los canales de la cuenta	Enumeración			
ListDatasetContents	Enumera información sobre el contenido de conjunto de datos que se ha creado	Enumeración	dataset*		
ListDatasets	Muestra los conjuntos de datos de la cuenta	Enumeración			
ListDatastores	Enumera los almacenes de datos de la cuenta	Enumeración			
ListPipelines	Enumera las canalizaciones de la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Muestra una lista de las etiquetas (metadatos) que se han asignado al recurso	Lectura	channel		
			dataset		
			datastore		
			pipeline		
PutLoggingOptions	Pone opciones de registro para la cuenta	Escritura			
RunPipelineActivity	Ejecuta la actividad de la canalización especificada	Lectura			
SampleChannelData	Muestras los datos del canal especificado	Lectura	channel*		
StartPipelineReprocessing	Comienza el reprocesado de la canalización especificada	Escritura	pipeline*		
TagResource	Agrega o modifica las etiquetas del recurso especificado. Las etiquetas son metadatos que se pueden utilizar para administrar un recurso.	Etiquetado	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Elimina la etiquetas especificadas (metadatos) del recurso	Etiquetado	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateChannel	Actualiza el canal especificado	Escritura	channel*		
UpdateDataset	Actualiza el conjunto de datos especificado	Escritura	dataset*		
UpdateDatastore	Actualiza el almacén de datos especificado	Escritura	datastore*		
UpdatePipeline	Actualiza la canalización especificada	Escritura	pipeline*		

Tipos de recursos definidos por AWS IoT Analytics

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
channel	`arn:${Partition}:iotanalytics:${Region}:${Account}:channel/${ChannelName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
dataset	`arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
datastore	`arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/${DatastoreName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/${PipelineName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}

Claves de condición para AWS IoT Analytics

AWS IoT Analytics define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
iotanalytics:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena

Acciones, recursos y claves de condición para AWS IoT Core Device Advisor

AWS IoT Core Device Advisor (prefijo de servicio:`iotdeviceadvisor`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Core Device Advisor
- Tipos de recursos definidos por AWS IoT Core Device Advisor
- Claves de condición para AWS IoT Core Device Advisor

Acciones definidas por AWS IoT Core Device Advisor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSuiteDefinition	Otorga permiso para crear una definición de conjunto.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSuiteDefinition	Otorga permiso para eliminar una definición de conjunto.	Escritura	Suitedefinition*		
GetEndpoint	Otorga permiso para obtener un punto de conexión de Device Advisor	Lectura			
GetSuiteDefinition	Otorga permiso para obtener una definición de conjunto.	Read	Suitedefinition*		
GetSuiteRun	Otorga permiso para obtener una ejecución de un conjunto.	Read	Suiterun*		
GetSuiteRunReport	Otorga permiso para obtener el informe de cualificación	Read	Suiterun*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	para una ejecución de un conjunto.				
ListSuiteDefinitions	Otorga permiso para enumerar definiciones de conjuntos.	List			
ListSuiteRuns	Otorga permiso para enumerar ejecuciones de conjuntos.	List	Suitedefinition*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas (metadatos) asignadas a un recurso.	Read	Suitedefinition		
			Suiterun		
StartSuiteRun	Otorga permisos para comenzar una ejecución de un conjunto.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopSuiteRun	Otorga permiso para detener una ejecución de un conjunto	Write	Suiterun*		
TagResource	Otorga permiso para agregar o modificar las etiquetas del recurso especificado. Las etiquetas son metadatos que se pueden utilizar para administrar un recurso.	Etiquetado	Suitedefinition		
			Suiterun		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar las etiquetas (metadatos) dadas de un recurso.	Etiquetado	Suitedefinition		
			Suiterun		
				aws:TagKeys	
UpdateSuiteDefinition	Otorga permiso para actualizar una definición de conjunto.	Write	Suitedefinition*		

Tipos de recursos definidos por AWS IoT Core Device Advisor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Suitedefinition	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suitedefinition/${SuiteDefinitionId}`	aws:ResourceTag/${TagKey}
Suiterun	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suiterun/${SuiteDefinitionId}/${SuiteRunId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT Core Device Advisor

AWS IoT Core Device Advisor define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS IoT Device Tester

AWS IoT Device Tester (prefijo de servicio:`iot-device-tester`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Device Tester
- Tipos de recursos definidos por AWS IoT Device Tester
- Claves de condición para AWS IoT Device Tester

Acciones definidas por AWS IoT Device Tester

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CheckVersion	Concede permiso a IoT Device Tester para comprobar si un conjunto determinado de versiones de producto, conjunto de pruebas y probador de dispositivos son compatibles	Lectura			
DownloadTestSuite	Concede permiso a IoT Device Tester para descargar	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	versiones compatibles del conjunto de pruebas				
LatestIdt	Concede permiso a IoT Device Tester para obtener información sobre la última versión disponible del probador de dispositivos	Lectura			
SendMetrics	Concede permiso a IoT Device Tester para enviar métricas de uso en su nombre	Escritura			
Supported Version	Concede permiso a IoT Device Tester para obtener una lista de versiones de productos y del conjunto de pruebas compatibles	Lectura			

Tipos de recursos definidos por AWS IoT Device Tester

AWS IoT Device Tester no admite la especificación de un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso a AWS IoT Device Tester, especifique `"Resource": "*"` en su política.

Claves de condición para AWS IoT Device Tester

IoT Device Tester no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS IoT Events

AWS IoT Events (prefijo de servicio:`iotevents`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Events
- Tipos de recursos definidos por AWS IoT Events
- Claves de condición para AWS IoT Events

Acciones definidas por AWS IoT Events

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchAcknowledgeAlarm	Otorga permiso para enviar una o más solicitudes de acuse de recibo a AWS IoT Events	Escritura	alarmModel*		
BatchDeleteDetector	Otorga permiso para eliminar una instancia de detector dentro del sistema AWS IoT Events	Escritura	detectorModel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDisableAlarm	Concede permiso para desactivar una o más instancias de alarma.	Write	alarmModel*		
BatchEnableAlarm	Concede permiso para habilitar una o más instancias de alarma.	Escritura	alarmModel*		
BatchPutMessage	Otorga permiso para enviar un conjunto de mensajes al sistema AWS IoT Events	Escritura	input*		
BatchResetAlarm	Concede permiso para restablecer una o más instancias de alarma.	Write	alarmModel*		
BatchSnoozeAlarm	Concede permiso para cambiar una o más instancias de alarma al modo posponer.	Escritura	alarmModel*		
BatchUpdateDetector	Otorga permiso para actualizar una instancia de detector dentro del sistema AWS IoT Events	Escritura	detectorModel*		
CreateAlarmModel	Otorga permiso para crear un modelo de alarma para monitorear un atributo de entrada de AWS IoT Events o una propiedad de un SiteWise activo de AWS IoT	Escritura	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDetectorModel	Otorga permiso para crear un modelo de detector para monitorear un atributo de entrada de AWS IoT Events	Escritura	detectorModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Otorga permiso para crear una entrada IotEvents	Escritura	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmModel	Concede permiso para eliminar un modelo de alarma.	Write	alarmModel*		
DeleteDetectorModel	Concede permiso para eliminar un modelo de detector.	Write	detectorModel*		
DeleteInput	Da permiso para eliminar una entrada.	Write	input*		
DescribeAlarm	Concede permiso para obtener información acerca de una instancia de alarma.	Read	alarmModel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAlarmModel	Concede permiso para obtener información acerca de un modelo de alarma.	Read	alarmModel*		
DescribeDetector	Concede permiso para obtener información acerca de una instancia de detector.	Read	detectorModel*		
DescribeDetectorModel	Concede permiso para obtener información acerca de un modelo de detector.	Lectura	detectorModel*		
DescribeDetectorModelAnalysis	Concede permiso para obtener información acerca del análisis del modelo de detector	Lectura			
DescribeInput	Concede permiso para obtener información acerca de la entrada.	Lectura	input*		
DescribeLoggingOptions	Otorga permiso para recuperar la configuración actual de las opciones de registro de AWS IoT Events	Lectura			
GetDetectorModelAnalysisResults	Concede permiso para recuperar los resultados del análisis del modelo de detector	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAlarmModelVersions	Concede permiso para enumerar todas las versiones de un modelo de alarma.	List	alarmModel*		
ListAlarmModels	Concede permiso para enumerar los modelos de alarmas que ha creado.	List			
ListAlarms	Concede permiso para obtener información acerca de todas las instancias de alarma por alarmModel.	List	alarmModel*		
ListDetectorModelVersions	Concede permiso para enumerar todas las versiones de un modelo de detector.	List	detectorModel*		
ListDetectorModels	Concede permiso para enumerar los modelos de detector que ha creado.	List			
ListDetectors	Concede permiso para obtener información acerca de todas las instancias de detector por detectormodel.	List	detectorModel*		
ListInputRoutings	Concede permiso para enumerar una o varias rutas de entrada	List			
ListInputs	Concede permiso para enumerar las entradas que ha creado.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas (metadatos) que ha asignado al recurso.	Lectura	alarmModel		
			detectorModel		
			input		
PutLoggingOptions	Otorga permiso para configurar o actualizar las opciones de registro de AWS IoT Events	Escritura			
StartDetectorModelAnalysis	Concede permiso para iniciar el análisis del modelo de detección	Escritura			
TagResource	Concede permiso para agregar o modificar las etiquetas del recurso especificado. Las etiquetas son metadatos que se pueden utilizar para administrar un recurso.	Etiquetado	alarmModel		
			detectorModel		
			input		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas (metadatos) dadas del recurso.	Etiquetado	alarmModel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			detectorModel		
			input		
				aws:TagKeys	
UpdateAlarmModel	Concede permiso para actualizar un modelo de alarma.	Write	alarmModel*		
UpdateDetectorModel	Concede permiso para actualizar un modelo de detector.	Write	detectorModel*		
UpdateInput	Da permiso para actualizar una entrada.	Write	input*		
UpdateInputRouting	Concede permiso para actualizar el direccionamiento de entrada.	Write	input*		

Tipos de recursos definidos por AWS IoT Events

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
detectorModel	`arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${DetectorModelName}`	aws:ResourceTag/${TagKey}
alarmModel	`arn:${Partition}:iotevents:${Region}:${Account}:alarmModel/${AlarmModelName}`	aws:ResourceTag/${TagKey}
input	`arn:${Partition}:iotevents:${Region}:${Account}:input/${InputName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT Events

AWS IoT Events define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso	Cadena
aws:TagKeys	Filtra las acciones por las claves de etiqueta en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
iotevents:keyValue	Filtra el acceso por el instanceId (clave-valor) del mensaje.	Cadena

Acciones, recursos y claves de condición para AWS IoT Fleet Hub para la administración de dispositivos

AWS IoT Fleet Hub for Device Management (prefijo de servicio:`iotfleethub`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Fleet Hub para la administración de dispositivos
- Tipos de recursos definidos por AWS IoT Fleet Hub para la administración de dispositivos
- Claves de condición para AWS IoT Fleet Hub para la administración de dispositivos

Acciones definidas por AWS IoT Fleet Hub para la administración de dispositivos

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Concede permiso para crear una aplicación.	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
DeleteApplication	Concede permiso para eliminar una aplicación.	Write	application*		sso:DeleteManagedApplicationInstance
DescribeApplication	Concede el permiso para describir una aplicación.	Read	application*		
ListApplications	Concede el permiso para enumerar todas las aplicaciones.	List			
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas para un recurso	Read	application		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	application		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	application		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Write	application*		

Tipos de recursos definidos por AWS IoT Fleet Hub para la administración de dispositivos

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:iotfleethub:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT Fleet Hub para la administración de dispositivos

AWS IoT Fleet Hub for Device Management define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso	Cadena
aws:TagKeys	Filtra las acciones por las claves de etiqueta en la solicitud	ArrayOfString

Claves de condiciones, recursos y acciones para el AWS IoT FleetWise

AWS IoT FleetWise (prefijo de servicio:`iotfleetwise`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el AWS IoT FleetWise
- Tipos de recursos definidos por el AWS IoT FleetWise
- Claves de condición para AWS IoT FleetWise

Acciones definidas por el AWS IoT FleetWise

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateVehicleFleet	Otorga permiso para asociar el vehículo determinado a una flota.	Escritura	fleet*		
			vehicle*		
CreateCampaign	Otorga permiso para crear una campaña	Escritura	campaign*		
			fleet*		
			signalcatalog*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys iotfleetwise:DestinationArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDecoderManifest	Otorga permiso para crear un manifiesto de decodificador para un modelo existente.	Escritura	decodermanifest*		
			modelmanifest*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleet	Otorga permiso para crear una flota.	Escritura	fleet*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelManifest	Otorga permiso para crear una definición de manifiesto del modelo	Escritura	modelmanifest*		
			signalcatalog*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalCatalog	Otorga permiso para crear un catálogo de señalización.	Escritura	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateTemplate	Otorga permiso para crear una plantilla de estado	Escritura	signalcatalog*		
			statetemplate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVehicle	Otorga permiso para crear un vehículo.	Escritura	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCampaign	Otorga permiso para eliminar una campaña	Escritura	campaign*		
DeleteDecoderManifest	Otorga permiso para eliminar el manifiesto de decodificador determinado	Escritura	decodermanifest*		
DeleteFleet	Otorga permiso para eliminar una flota.	Escritura	fleet*		
DeleteModelManifest	Otorga permiso para eliminar el manifiesto de modelo determinado.	Escritura	modelmanifest*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSignalCatalog	Otorga permiso para eliminar un catálogo de señalización específico.	Escritura	signalcatalog*		
DeleteStateTemplate	Otorga permiso para eliminar una plantilla de estado	Escritura	statetemplate*		
DeleteVehicle	Otorga permiso para eliminar un vehículo.	Escritura	vehicle*		
DisassociateVehicleFleet	Otorga permiso para desasociar un vehículo de una flota existente.	Escritura	fleet*		
			vehicle*		
GenerateCommandPayload [solo permiso]	Otorga permiso para generar la carga útil necesaria para ejecutar un comando en un vehículo	Administración de permisos	vehicle*		
			statetemplate		
				iotfleetwise:Signals	
GetCampaign	Otorga permiso para obtener información resumida de una campaña determinada.	Lectura	campaign*		
GetDecoderManifest	Otorga permiso para obtener información resumida para una definición de manifiesto de decodificador determinada.	Lectura	decodermanifest*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEncryptionConfiguration	Otorga permiso para obtener el estado de cifrado basado en KMS para el Cuenta de AWS	Lectura			
GetFleet	Otorga permiso para obtener información resumida sobre una flota.	Lectura	fleet*		
GetLoggingOptions	Otorga permiso para obtener las opciones de registro de Cuenta de AWS	Lectura			
GetModelManifest	Otorga permiso para obtener información resumida de una definición de manifiesto de modelo determinada.	Lectura	modelmanifest*		
GetRegisterAccountStatus	Otorga permiso para obtener el estado de registro de la cuenta con IoT FleetWise	Lectura			
GetSignalCatalog	Otorga permiso para obtener información resumida de un catálogo de señalización específico.	Lectura	signalcatalog*		
GetStateTemplate	Otorga permiso para obtener información resumida para una plantilla de estado determinada	Lectura	statetemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVehicle	Otorga permiso para obtener información resumida sobre un vehículo.	Lectura	vehicle*		
GetVehicleStatus	Otorga permiso para obtener el estado de las campañas en ejecución en un vehículo específico.	Lectura	vehicle*		
ImportDecoderManifest	Concede el permiso para eliminar un manifiesto de decodificador existente.	Escritura	decodermanifest*		
ImportSignalCatalog	Otorga permiso para crear un catálogo de señalizaciones mediante la importación de definiciones existentes.	Escritura	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCampaigns	Otorga permiso para enumerar campañas	Lectura			
ListDecoderManifestNetworkInterfaces	Otorga permiso para enumerar las interfaces de red asociadas al manifiesto de decodificador existente.	Enumeración	decodermanifest*		
ListDecoderManifestSignals	Otorga permiso para enumerar señalizaciones de manifiesto de decodificador.	Enumeración	decodermanifest*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDecoderManifests	Otorga permiso para enumerar todos los manifiestos de decodificador, con un filtro opcional en el manifiesto del modelo.	Lectura			
ListFleets	Otorga permiso para enumerar todas las flotas.	Lectura			
ListFleetsForVehicle	Otorga permiso para enumerar todas las flotas a las que está asociado el vehículo especificado.	Lectura	vehicle*		
ListModelManifestNodes	Otorga permiso para enumerar todos los nodos para el manifiesto de modelo determinado.	Enumeración	modelmanifest*		
ListModelManifests	Otorga permiso para enumerar todos los manifiestos de modelo, con un filtro opcional en el catálogo de señalización.	Lectura			
ListSignalCatalogNodes	Otorga permiso para enumerar todos los notos de un catálogo de señalización determinado.	Lectura	signalcatalog*		
ListSignalCatalogs	Otorga permiso para enumerar todos los catálogos de señalización.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStateTemplates	Otorga permiso para enumerar plantillas de estados	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
ListVehicles	Otorga permiso para enumerar todos los vehículos, con un filtro opcional en el manifiesto del modelo.	Lectura			
ListVehiclesInFleet	Otorga permiso para enumerar vehículos en una flota determinada.	Lectura	fleet*		
PutEncryptionConfiguration	Otorga permiso para habilitar o deshabilitar el cifrado basado en KMS para Cuenta de AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutLoggingOptions	Otorga permiso para colocar las opciones de registro para el Cuenta de AWS	Escritura			
RegisterAccount	Otorga permiso para registrarse y Cuenta de AWS para IoT FleetWise	Escritura			iam:PassRole
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource		Etiquetado	campaign		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para eliminar etiquetas de un recurso		decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:TagKeys	
UpdateCampaign	Otorga permiso para actualizar una campaña determinada.	Escritura	campaign*		
UpdateDecoderManifest	Otorga permiso para actualizar una definición de manifiesto de decodificador.	Escritura	decodermanifest*		
UpdateFleet	Otorga permiso para actualizar la flota.	Escritura	fleet*		
UpdateModelManifest	Otorga permiso para actualizar la definición de manifiesto de modelo determinada.	Escritura	modelmanifest*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSignalCatalog	Otorga permiso para actualizar una definición de catálogo de señalización específica.	Escritura	signalcatalog*		
UpdateStateTemplate	Otorga permiso para actualizar la plantilla de estado en cuestión	Escritura	statetemplate*		
UpdateVehicle	Otorga permiso para actualizar el vehículo.	Escritura	vehicle*		
			decodermanifest		
			modelmanifest		
				iotfleetwise:UpdateToModelManifestArn iotfleetwise:UpdateToDecoderManifestArn	

Tipos de recursos definidos por el AWS IoT FleetWise

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
campaign	`arn:${Partition}:iotfleetwise:${Region}:${Account}:campaign/${CampaignName}`	aws:ResourceTag/${TagKey}
decodermanifest	`arn:${Partition}:iotfleetwise:${Region}:${Account}:decoder-manifest/${Name}`	aws:ResourceTag/${TagKey}
fleet	`arn:${Partition}:iotfleetwise:${Region}:${Account}:fleet/${FleetId}`	aws:ResourceTag/${TagKey}
modelmanifest	`arn:${Partition}:iotfleetwise:${Region}:${Account}:model-manifest/${Name}`	aws:ResourceTag/${TagKey}
signalcatalog	`arn:${Partition}:iotfleetwise:${Region}:${Account}:signal-catalog/${Name}`	aws:ResourceTag/${TagKey}
vehicle	`arn:${Partition}:iotfleetwise:${Region}:${Account}:vehicle/${VehicleId}`	aws:ResourceTag/${TagKey}
statetemplate	`arn:${Partition}:iotfleetwise:${Region}:${Account}:state-template/${StateTemplateId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT FleetWise

AWS El IoT FleetWise define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
iotfleetwise:DestinationArn	Filtra el acceso en función del ARN de destino de la campaña, como, por ejemplo, un ARN de bucket de S3 o un ARN de Timestream	ARN
iotfleetwise:Signals	Filtra el acceso mediante nombres de señal totalmente cualificados	ArrayOfString
iotfleetwise:UpdateToDecoderManifestArn	Filtra el acceso mediante una lista de IoT FleetWise Decoder Manifest ARNs	ARN
iotfleetwise:UpdateToModelManifestArn	Filtra el acceso mediante una lista del manifiesto del FleetWise modelo de IoT ARNs	ARN

Acciones, recursos y claves de condición para AWS IoT Greengrass

AWS IoT Greengrass (prefijo de servicio:`greengrass`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Greengrass
- Tipos de recursos definidos por AWS IoT Greengrass
- Claves de condición para AWS IoT Greengrass

Acciones definidas por AWS IoT Greengrass

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate RoleToGroup	Concede permiso para asociar un rol a un grupo. Los permisos del rol deben permitir que las funciones y los conectores principales de Lambda de Greengrass realicen acciones en otros servicios AWS	Escritura	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateServiceRoleToAccount	Otorga permiso para asociar un rol a su cuenta. AWS IoT Greengrass utiliza esta función para acceder a sus funciones de Lambda y sus recursos de IoT. AWS	Administración de permisos			
CreateConnectorDefinition	Concede permiso para crear una definición de conector	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorDefinitionVersion	Concede permiso para crear una versión de una definición de conector existente	Write	connectorDefinition*		
CreateCoreDefinition	Concede permiso para crear una definición de núcleo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	Concede permiso para crear una versión de una definición de núcleo existente. Los grupos de Greengrass deben contener exactamente un núcleo de Greengrass cada uno	Write	coreDefinition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeployment	Concede permiso para crear una implementación.	Write	group*		
CreateDeviceDefinition	Concede permiso para crear una definición de dispositivo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	Concede permiso para crear una versión de una definición de dispositivo existente	Write	deviceDefinition*		
CreateFunctionDefinition	Concede permiso para crear una definición de función de Lambda que se pueda utilizar en un grupo que contenga una lista de funciones de Lambda y sus configuraciones	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	Concede permiso para crear una versión de una definición de función de Lambda existente	Escritura	functionDefinition*		
CreateGroup	Concede permiso para crear un grupo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGroupCertificateAuthority	Concede permiso para crear una CA para el grupo o rotar la CA actual	Write	group*		
CreateGroupVersion	Concede permiso para crear una versión de un grupo que ya se ha definido	Write	group*		
CreateLoggerDefinition	Concede permiso para crear una definición de registrador	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	Concede permiso para crear una versión de una definición de registrador existente	Write	loggerDefinition*		
CreateResourceDefinition	Concede permiso para crear una definición de recursos que contenga una lista de los recursos que se utilizarán en un grupo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDefinitionVersion	Concede permiso para crear una versión de una definición de recursos existente	Escritura	resourceDefinition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSoftwareUpdateJob	Otorga permiso para crear un trabajo de AWS IoT que activará sus núcleos de Greengrass para que actualicen el software que están ejecutando	Escritura			
CreateSubscriptionDefinition	Concede permiso para crear una definición de suscripción	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	Concede permiso para crear una versión de una definición de suscripción existente	Write	subscriptionDefinition*		
DeleteConnectorDefinition	Concede permiso para eliminar una definición de conector	Write	connectorDefinition*		
DeleteCoreDefinition	Concede permiso para eliminar una definición de núcleo. La eliminación de una definición que se encuentra en uso en una implementación afecta a futuras implementaciones	Write	coreDefinition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDeviceDefinition	Concede permiso para eliminar una definición de dispositivo. La eliminación de una definición que se encuentra en uso en una implementación afecta a futuras implementaciones	Write	deviceDefinition*		
DeleteFunctionDefinition	Concede permiso para eliminar una definición de función Lambda. La eliminación de una definición que se encuentra en uso en una implementación afecta a futuras implementaciones	Write	functionDefinition*		
DeleteGroup	Concede permiso para eliminar un grupo que actualmente no se usa en una implementación	Write	group*		
DeleteLoggerDefinition	Concede permiso para eliminar una definición de registrador. La eliminación de una definición que se encuentra en uso en una implementación afecta a futuras implementaciones	Write	loggerDefinition*		
DeleteResourceDefinition	Concede permiso para eliminar una definición de recursos	Write	resourceDefinition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSubscriptionDefinition	Concede permiso para eliminar una definición de suscripción. La eliminación de una definición que se encuentra en uso en una implementación afecta a futuras implementaciones	Write	subscriptionDefinition*		
DisassociateRoleFromGroup	Concede permiso para desasociar el rol de un grupo	Write	group*		
DisassociateServiceRoleFromAccount	Concede permiso para desasociar el rol de servicio de una cuenta. Sin un rol de servicio, las implementaciones no funcionarán	Write			
Discover	Concede permiso para recuperar la información necesaria para conectarse a un núcleo de Greengrass	Read	thing*		
GetAssociatedRole	Concede permiso para recuperar el rol asociado a un grupo	Read	group*		
GetBulkDeploymentStatus	Concede permiso para devolver el estado de una implementación masiva	Read	bulkDeployment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnectivityInfo	Concede permiso para recuperar información de conectividad para un núcleo	Read	connectivityInfo*		
GetConnectorDefinition	Concede permiso para recuperar información sobre una definición de conector	Read	connectorDefinition*		
GetConnectorDefinitionVersion	Concede permiso para recuperar información sobre una versión de definición de conector	Read	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	Concede permiso para recuperar información sobre una definición de núcleo	Read	coreDefinition*		
GetCoreDefinitionVersion	Concede permiso para recuperar información sobre una versión de definición de núcleo	Read	coreDefinition*		
			coreDefinitionVersion*		
GetDeploymentStatus	Concede permiso para devolver el estado de una implementación	Read	deployment*		
			group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDeviceDefinition	Concede permiso para recuperar información sobre una definición de dispositivo	Read	deviceDefinition*		
GetDeviceDefinitionVersion	Concede permiso para recuperar información sobre una versión de definición de dispositivo	Read	deviceDefinition*		
			deviceDefinitionVersion*		
GetFunctionDefinition	Concede permiso para recuperar información sobre una definición de función de Lambda, como su hora de creación y versión más reciente	Read	functionDefinition*		
GetFunctionDefinitionVersion	Concede permiso para recuperar información sobre una versión de definición de función de Lambda, como, por ejemplo, qué funciones de Lambda se incluyen en la versión y sus configuraciones	Read	functionDefinition*		
			functionDefinitionVersion*		
GetGroup	Concede permiso para recuperar información sobre un grupo	Read	group*		
GetGroupCertificateAuthority	Concede permiso para devolver la clave pública de la CA asociada a un grupo	Read	certificateAuthority*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			group*		
GetGroupCertificateConfiguration	Concede permiso para recuperar la configuración actual de la CA utilizada por un grupo	Read	group*		
GetGroupVersion	Concede permiso para recuperar información sobre una versión de grupo	Read	group*		
			groupVersion*		
GetLoggerDefinition	Concede permiso para recuperar información sobre una definición de registrador	Read	loggerDefinition*		
GetLoggerDefinitionVersion	Concede permiso para recuperar información sobre una versión de definición de registrador	Read	loggerDefinition*		
			loggerDefinitionVersion*		
GetResourceDefinition	Concede permiso para recuperar información sobre una definición de recursos, como su hora de creación y versión más reciente	Read	resourceDefinition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourceDefinitionVersion	Concede permiso para recuperar información sobre una versión de la definición de recursos, como, por ejemplo, qué recursos se incluyen en la versión	Read	resourceDefinition*		
			resourceDefinitionVersion*		
GetServiceRoleForAccount	Concede permiso para recuperar el rol de servicio que está adjuntado a una cuenta	Read			
GetSubscriptionDefinition	Concede permiso para recuperar información sobre una definición de suscripción	Read	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	Concede permiso para recuperar información sobre una versión de definición de suscripción	Read	subscriptionDefinition*		
			subscriptionDefinitionVersion*		
GetThingRuntimeConfiguration	Concede permiso para recuperar la configuración de tiempo de ejecución de una cosa	Read	thingRuntimeConfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBulkDeploymentDetailedReports	Concede permiso para recuperar un listado paginado de las implementaciones que se iniciaron en una operación de implementación masiva y su estado de implementación actual	Read	bulkDeployment*		
ListBulkDeployments	Concede permiso para recuperar una lista de implementaciones masivas	List			
ListConnectorDefinitionVersions	Concede permiso para obtener una lista de las versiones de una definición de conector	List	connectorDefinition*		
ListConnectorDefinitions	Concede permiso para recuperar una lista de definiciones de conectores	List			
ListCoreDefinitionVersions	Concede permiso para obtener una lista de las versiones de una definición de núcleo	List	coreDefinition*		
ListCoreDefinitions	Concede permiso para recuperar una lista de definiciones de núcleos	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeployments	Concede permiso para recuperar una lista de todas las implementaciones de un grupo	List	group*		
ListDeviceDefinitionVersions	Concede permiso para obtener una lista de las versiones de una definición de dispositivos	List	deviceDefinition*		
ListDeviceDefinitions	Concede permiso para recuperar una lista de definiciones de dispositivos	List			
ListFunctionDefinitionVersions	Concede permiso para crear una lista de versiones de una definición de función de Lambda	List	functionDefinition*		
ListFunctionDefinitions	Concede permiso para recuperar una lista de definiciones de funciones de Lambda	Enumeración			
ListGroupCertificateAuthorities	Otorga permiso para recuperar una lista de los datos actuales CAs de un grupo	Enumeración	group*		
ListGroupVersions	Concede permiso para crear una lista de las versiones de un grupo	List	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGroups	Concede permiso para recuperar una lista de grupos	List			
ListLoggerDefinitionVersions	Concede permiso para crear una lista de versiones de una definición de registrador	List	loggerDefinition*		
ListLoggerDefinitions	Concede permiso para recuperar una lista de definiciones de registrador	List			
ListResourceDefinitionVersions	Concede permiso para crear una lista de las versiones de una definición de recursos	List	resourceDefinition*		
ListResourceDefinitions	Concede permiso para recuperar una lista de definiciones de recursos	List			
ListSubscriptionDefinitionVersions	Concede permiso para obtener una lista de versiones de una definición de suscripción	List	subscriptionDefinition*		
ListSubscriptionDefinitions	Concede permiso para recuperar una lista de definiciones de suscripciones	List			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Read	bulkDeployment		
			connectorDefinition		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetDeployments	Concede permiso para restablecer las implementaciones de un grupo	Write	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartBulkDeployment	Concede permiso para implementar varios grupos en una operación	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	Concede permiso para detener la ejecución de una implementación masiva	Write	bulkDeployment*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	Concede permiso para actualizar la información de conectividad de un núcleo de Greengrass. Los dispositivos que pertenezcan al grupo que tiene este núcleo recibirán esta información para poder encontrar la ubicación del núcleo y conectarse a este	Write	connectivityInfo*		
UpdateConnectorDefinition	Concede permiso para actualizar una definición de conector	Write	connectorDefinition*		
UpdateCoreDefinition	Concede permiso para actualizar una definición de núcleo	Write	coreDefinition*		
UpdateDeviceDefinition	Concede permiso para actualizar una definición de dispositivo	Write	deviceDefinition*		
UpdateFunctionDefinition	Concede permiso para actualizar una definición de función de Lambda	Write	functionDefinition*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGroup	Concede permiso para actualizar un grupo	Write	group*		
UpdateGroupCertificateConfiguration	Concede permiso para actualizar el tiempo de caducidad del certificado para un grupo	Write	group*		
UpdateLoggerDefinition	Concede permiso para actualizar una definición de registrador	Write	loggerDefinition*		
UpdateResourceDefinition	Concede permiso para actualizar una definición de recursos	Write	resourceDefinition*		
UpdateSubscriptionDefinition	Concede permiso para actualizar una definición de suscripción	Write	subscriptionDefinition*		
UpdateThingRuntimeConfiguration	Concede permiso para actualizar la configuración de tiempo de ejecución de una cosa	Write	thingRuntimeConfig*		

Tipos de recursos definidos por AWS IoT Greengrass

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
connectivityInfo	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo	
certificateAuthority	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/certificateauthorities/${CertificateAuthorityId}	
deployment	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}	
bulkDeployment	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}	aws:ResourceTag/${TagKey}
group	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}	aws:ResourceTag/${TagKey}
groupVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}	
coreDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}	aws:ResourceTag/${TagKey}
coreDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}/versions/${VersionId}	

Tipos de recurso	ARN	Claves de condición
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}
deviceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}	
functionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}	aws:ResourceTag/${TagKey}
functionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}	
subscriptionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}	aws:ResourceTag/${TagKey}
subscriptionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}/versions/${VersionId}	
loggerDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
loggerDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}/versions/${VersionId}	
resourceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}	aws:ResourceTag/${TagKey}
resourceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}/versions/${VersionId}	
connectorDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}	aws:ResourceTag/${TagKey}
connectorDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}/versions/${VersionId}	
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
thingRuntimeConfig	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/runtimeconfig	

Claves de condición para AWS IoT Greengrass

AWS IoT Greengrass define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas obligatorias	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS IoT Greengrass V2

AWS IoT Greengrass V2 (prefijo de servicio:`greengrass`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Greengrass V2
- Tipos de recursos definidos por AWS IoT Greengrass V2
- Claves de condición para AWS IoT Greengrass V2

Acciones definidas por AWS IoT Greengrass V2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateServiceRoleToAccount	Otorga permiso para asociar un rol a su cuenta. AWS IoT Greengrass utiliza esta función para acceder a sus funciones de Lambda y sus recursos de IoT. AWS	Administración de permisos			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	Concede permiso para asociar una lista de dispositivos cliente a un dispositivo principal.	Escritura	coreDevice*		
BatchDisassociateClientDeviceFromCoreDevice	Otorga permiso para disociar una lista de dispositivos cliente a un dispositivo principal.	Escritura	coreDevice*		
CancelDeployment	Concede permiso para cancelar una implementación.	Escritura	deployment*		iot:CancelJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	Concede permiso para crear un componente.	Write	component * aws:RequestTag/${TagKey} aws:TagKeys		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeployment	Concede permiso para crear una implementación.	Write		aws:RequestTag/${TagKey} aws:TagKeys	iot:CancelJob iot:CreateJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
DeleteComponent	Concede el permiso para eliminar un componente.	Escritura	componentVersion*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCoreDevice	Otorga permiso para eliminar un dispositivo principal de AWS IoT Greengrass, que es cosa de AWS IoT. Esta operación elimina el dispositivo central de la lista de dispositivos centrales. Esta operación no elimina lo del AWS IoT	Escritura	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	Concede permiso para eliminar una implementación. Para eliminar una implementación activa, primero debe cancelarse	Escritura	deployment*		iot:DeleteJob
DescribeComponent	Concede permiso para recuperar metadatos de una versión de un componente.	Lectura	componentVersion*		
DisassociateServiceRoleFromAccount	Concede permiso para desasociar el rol de servicio de una cuenta. Sin un rol de servicio, las implementaciones no funcionarán	Escritura			
GetComponent	Concede permiso para obtener la receta de una versión de un componente.	Lectura	componentVersion*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetComponentVersionArtifact	Concede permiso para obtener la URL prefirmada para descargar un artefacto de componente público	Lectura	componentVersion*		
GetConnectivityInfo	Concede permiso para recuperar información de conectividad para un dispositivo central de Greengrass	Lectura	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	Otorga permiso para recuperar los metadatos de un dispositivo central de AWS IoT Greengrass	Lectura	coreDevice*		
GetDeployment	Concede permiso para obtener una implementación.	Lectura	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	Concede permiso para recuperar el rol de servicio que está adjuntado a una cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListClientDevicesAssociatedWithCoreDevice	Otorga permiso para recuperar una lista paginada de dispositivos cliente asociados a un dispositivo principal de AWS IoT Greengrass	Enumeración	coreDevice*		
ListComponentVersions	Concede permiso para recuperar una lista paginada de todas las versiones de un componente.	List	component*		
ListComponents	Concede permiso para recuperar una lista paginada de los resúmenes de componentes.	Enumeración			
ListCoreDevices	Otorga permiso para recuperar una lista paginada de los AWS dispositivos principales de IoT Greengrass	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeployments	Concede permiso para recuperar una lista paginada de las implementaciones.	Enumeración			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListEffectiveDeployments	Otorga permiso para recuperar una lista paginada de los trabajos de despliegue que IoT AWS Greengrass envía a los dispositivos principales de IoT AWS Greengrass	Enumeración	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListInstalledComponents	Otorga permiso para recuperar una lista paginada de los componentes que ejecuta un dispositivo AWS principal de IoT Greengrass	Enumeración	coreDevice*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	Concede permiso para enumerar los componentes que cumplen los requisitos de componente, versión y plataforma de una implementación.	List	componentVersion*		
TagResource	Otorga permiso para agregar etiquetas a un recurso.	Etiquetado	component		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConnectivityInfo	Concede permiso para actualizar la información de conectividad de un núcleo de Greengrass. Los dispositivos que pertenezcan al grupo que tiene este núcleo recibirán esta información para poder encontrar la ubicación del núcleo y conectarse a este	Escritura	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

Tipos de recursos definidos por AWS IoT Greengrass V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
component	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
componentVersion	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}:versions:${ComponentVersion}`	aws:ResourceTag/${TagKey}
coreDevice	`arn:${Partition}:greengrass:${Region}:${Account}:coreDevices:${CoreDeviceThingName}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:deployments:${DeploymentId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT Greengrass V2

AWS IoT Greengrass V2 define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso comprobando los key/value pares de etiquetas incluidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso comprobando los key/value pares de etiquetas asociados a un recurso específico	Cadena
aws:TagKeys	Filtra el acceso mediante la verificación de claves de etiquetas que se pasan en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para los trabajos de AWS IoT DataPlane

AWS IoT Jobs DataPlane (prefijo de servicio:`iotjobsdata`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Jobs DataPlane
- Tipos de recursos definidos por los trabajos de AWS IoT DataPlane
- Claves de condición para trabajos de AWS IoT DataPlane

Acciones definidas por AWS IoT Jobs DataPlane

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeJobExecution	Concede permiso para describir una ejecución de trabajo	Lectura	thing*		
				iot:JobId	
GetPendingJobExecutions	Otorga permiso para obtener la lista de todos los trabajos para un objeto que no está en un estado terminal	Lectura	thing*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartNextPendingJobExecution	Otorga permiso para obtener e iniciar la próxima ejecución de trabajo pendiente para un objeto	Escritura	thing*		
UpdateJobExecution	Otorga permiso para actualizar una ejecución de trabajo	Escritura	thing*		
				iot:JobId	

Tipos de recursos definidos por los trabajos de AWS IoT DataPlane

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	

Claves de condición para trabajos de AWS IoT DataPlane

AWS IoT Jobs DataPlane define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
iot:JobId	Filtra el acceso de JoBid para iotjobsdata: e iotjobsdata: DescribeJobExecution UpdateJobExecution APIs	Cadena

Claves de condiciones, recursos y acciones para las integraciones gestionadas de AWS IoT

AWS Las integraciones gestionadas de IoT (prefijo de servicio:`iotmanagedintegrations`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las integraciones gestionadas de AWS IoT
- Tipos de recursos definidos por las integraciones gestionadas de AWS IoT
- Claves de condición para las integraciones gestionadas de AWS IoT

Acciones definidas por las integraciones gestionadas de AWS IoT

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccountAssociation	Otorga permiso para crear una nueva asociación de cuentas	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudConnector	Otorga permiso para crear un nuevo conector de nube	Escritura			
CreateConnectorDestination	Otorga permiso para crear un nuevo destino de conector	Escritura			
CreateCredentialLocker	Otorga permiso para crear un casillero de credenciales de producto	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDestination	Otorga permiso para crear un nuevo destino	Escritura			
CreateEventLogConfiguration	Otorga permiso para crear una nueva configuración de eventos	Escritura			
CreateManagedThing	Otorga permiso para crear un nuevo elemento gestionado	Escritura	credential-locker		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateNotificationConfiguration	Otorga permiso para crear una nueva configuración de notificaciones	Escritura			
CreateOtaTask	Otorga permiso para crear una nueva tarea ota	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOtaTaskConfiguration	Otorga permiso para crear una nueva configuración de tareas ota	Escritura			
CreateProvisioningProfile	Otorga permiso para crear un nuevo perfil de aprovisionamiento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssociation	Otorga permiso para eliminar una asociación de cuentas	Escritura	account-association*		
DeleteCloudConnector	Otorga permiso para eliminar un conector de nube	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConnectorDestination	Otorga permiso para eliminar el destino de un conector	Escritura			
DeleteCredentialLocker	Otorga permiso para eliminar un casillero de credenciales	Escritura	credential-locker*		
DeleteDestination	Otorga permiso para eliminar un destino	Escritura			
DeleteEventLogConfiguration	Otorga permiso para eliminar la configuración del registro de eventos	Escritura			
DeleteManagedThing	Otorga permiso para eliminar lo gestionado	Escritura	managed-thing*		
DeleteNotificationConfiguration	Otorga permiso para eliminar la configuración de notificaciones	Escritura			
DeleteOtaTask	Otorga permiso para eliminar una tarea	Escritura	ota-task*		
DeleteOtaTaskConfiguration	Otorga permiso para eliminar la configuración de la tarea ota	Escritura			
DeleteProvisioningProfile	Otorga permiso para eliminar el perfil de aprovisionamiento	Escritura	provisioning-profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterAccountAssociation	Otorga permiso para anular el registro de la asociación de cuentas	Escritura	account-association*		
			managed-thing*		
GetAccountAssociation	Otorga permiso para obtener información sobre una asociación de cuentas	Lectura	account-association*		
GetCloudConnector	Otorga permiso para obtener información sobre un conector en la nube	Lectura			
GetConnectorDestination	Otorga permiso para obtener información sobre un destino en la nube	Lectura			
GetCredentialLocker	Otorga permiso para obtener información sobre un depósito de credenciales	Lectura	credential-locker*		
GetCustomEndpoint	Otorga permiso para obtener información sobre un punto final personalizado	Lectura			
GetDefaultEncryptionConfiguration	Otorga permiso para obtener información sobre una configuración de cifrado predeterminada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDestination	Otorga permiso para obtener información sobre un destino	Lectura			
GetDeviceDiscovery	Otorga permiso para obtener información sobre el descubrimiento de un dispositivo	Lectura			
GetEventLogConfiguration	Otorga permiso para obtener información sobre la configuración de un registro de eventos	Lectura			
GetHubConfiguration	Otorga permiso para obtener información sobre la configuración de un hub	Lectura			
GetManagedThing	Otorga permiso para obtener información sobre un elemento gestionado	Lectura	managed-thing*		
GetManagedThingCapabilities	Otorga permiso para obtener el informe de capacidad de un elemento gestionado	Lectura	managed-thing*		
GetManagedThingConnectivityData	Otorga permiso para obtener los datos de conectividad de un dispositivo gestionado	Lectura	managed-thing*		
GetManagedThingMetaData	Otorga permiso para obtener la información de metadatos de un elemento gestionado	Lectura	managed-thing*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetManagedThingState	Otorga permiso para obtener la información de estado del dispositivo para un elemento gestionado	Lectura	managed-thing*		
GetNotificationConfiguration	Otorga permiso para obtener información para una configuración de notificaciones	Lectura			
GetOtaTask	Otorga permiso para obtener información para una tarea de OTA	Lectura	ota-task*		
GetOtaTaskConfiguration	Otorga permiso para obtener información para la configuración de una tarea ota	Lectura			
GetProvisioningProfile	Otorga permiso para obtener información para un perfil de aprovisionamiento	Lectura	provisioning-profile*		
GetRuntimeLogConfiguration	Otorga permiso para obtener información para una configuración de registro de tiempo de ejecución	Lectura			
GetSchemaVersion	Otorga permiso para obtener información para una versión de un esquema	Lectura			
ListAccountAssociations	Otorga permiso para incluir información para las asociaciones de cuentas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCloudConnectors	Otorga permiso para incluir información en los conectores de nube	Enumeración			
ListConnectorDestinations	Otorga permiso para incluir información sobre los destinos de los conectores	Enumeración			
ListCredentialLockers	Otorga permiso para incluir información para los casilleros de credenciales	Enumeración			
ListDestinations	Otorga permiso para incluir información sobre los destinos	Enumeración			
ListDeviceDiscoveries	Otorga permiso para incluir información a fin de detectar dispositivos	Enumeración			
ListDiscoveredDevices	Otorga permiso para incluir información sobre el dispositivo descubierto en un descubrimiento de dispositivos	Lectura			
ListEventLogConfigurations	Otorga permiso para incluir información para las configuraciones del registro de eventos	Lectura			
ListManagedThingAccountAssociations	Otorga permiso para incluir información sobre las asociaciones entre entidades gestionadas y asociaciones de cuentas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListManagedThingSchemas	Otorga permiso para enumerar los esquemas asociados a un elemento administrado	Lectura	managed-thing*		
ListManagedThings	Otorga permiso para enumerar la información de las cosas administradas	Enumeración			
ListNotificationConfigurations	Otorga permiso para incluir información para las configuraciones de notificaciones	Lectura			
ListOtaTaskConfigurations	Otorga permiso para incluir información para las configuraciones de tareas OTA	Lectura			
ListOtaTaskExecutions	Otorga permiso para incluir información para la ejecución de tareas ota	Lectura	ota-task*		
ListOtaTasks	Otorga permiso para incluir información para las tareas ota	Enumeración			
ListProvisioningProfiles	Otorga permiso para incluir información para los perfiles de aprovisionamiento	Enumeración			
ListSchemaVersions	Otorga permiso para incluir información para los esquemas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas del recurso especificado	Lectura	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		
				aws:ResourceTag/${TagKey}	
PutDefaultEncryptionConfiguration	Otorga permiso para actualizar la configuración predeterminada de una configuración de cifrado	Escritura			
PutHubConfiguration	Otorga permiso para actualizar la configuración de un hub	Escritura			
PutRuntimeLogConfiguration	Otorga permiso para actualizar una configuración de registro de tiempo de ejecución	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterAccountAssociation	Otorga permiso para registrar una asociación de cuentas a un elemento gestionado	Escritura	account-association*		
			managed-thing*		
RegisterCustomEndpoint	Otorga permiso para registrar un punto final personalizado	Escritura			
ResetRuntimeLogConfiguration	Otorga permiso para restablecer la configuración de un registro de tiempo de ejecución	Escritura			
SendConnectorEvent	Otorga permiso para enviar un evento de conector	Escritura			
SendManagedThingCommand	Otorga permiso para enviar un comando a un elemento gestionado	Escritura	managed-thing*		
			account-association		
StartAccountAssociationRefresh	Otorga permiso para iniciar una actualización de los tokens de acceso asociados a una asociación de cuentas	Escritura	account-association*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDeviceDiscovery	Otorga permiso para iniciar la detección de un dispositivo	Escritura	account-association		
			managed-thing		
TagResource	Otorga permiso para añadir etiquetas al recurso especificado	Etiquetado	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas del recurso especificado	Etiquetado	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccountAssociation	Otorga permiso para actualizar la asociación de una cuenta	Escritura	account-association*		
UpdateCloudConnector	Otorga permiso para actualizar un conector de nube	Escritura			
UpdateConnectorDestination	Otorga permiso para actualizar el destino de un conector	Escritura			
UpdateDestination	Otorga permiso para actualizar un destino.	Escritura			
UpdateEventLogConfiguration	Otorga permiso para actualizar la configuración de un registro de eventos	Escritura			
UpdateManagedThing	Otorga permiso para actualizar un elemento gestionado	Escritura	managed-thing* credential-locker		
UpdateNotificationConfiguration	Otorga permiso para actualizar una configuración de notificaciones	Escritura			
UpdateOtaTask	Otorga permiso para actualizar una tarea ota	Escritura	ota-task*		

Tipos de recursos definidos por las integraciones gestionadas de AWS IoT

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
account-association	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:account-association/${AccountAssociationId}`	aws:ResourceTag/${TagKey}
credential-locker	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:credential-locker/${Identifier}`	aws:ResourceTag/${TagKey}
managed-thing	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:managed-thing/${Identifier}`	aws:ResourceTag/${TagKey}
ota-task	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:ota-task/${Identifier}`	aws:ResourceTag/${TagKey}
provisioning-profile	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:provisioning-profile/${Identifier}`	aws:ResourceTag/${TagKey}

Claves de condición para las integraciones gestionadas de AWS IoT

AWS Las integraciones gestionadas de IoT definen las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condiciones, recursos y acciones para el AWS IoT SiteWise

AWS IoT SiteWise (prefijo de servicio:`iotsitewise`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el AWS IoT SiteWise
- Tipos de recursos definidos por el AWS IoT SiteWise
- Claves de condición para AWS IoT SiteWise

Acciones definidas por el AWS IoT SiteWise

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateAssets	Concede permiso para asociar un activo secundario a un activo principal a través de una jerarquía	Escritura	asset*		
AssociateTimeSeriesToAssetProperty	Concede permiso para asociar una serie temporal a una propiedad de activos	Escritura	asset* time-series*		
BatchAssociateProjectAssets	Concede permiso para asociar activos a un proyecto específico	Write	project*		
BatchDisassociateProjectAssets	Concede permiso para disociar activos de un proyecto específico	Escritura	project*		
BatchGetAssetPropertyAggregates	Concede permiso para recuperar agregados calculados para varias propiedades de activos	Lectura	asset time-series		
BatchGetAssetPropertyValue	Concede permiso para recuperar el valor más reciente para varias propiedades de activos	Lectura	asset time-series		
BatchGetAssetPrope	Concede permiso para recuperar el historial de	Lectura	asset		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
rtyValueHistory	valores más reciente para varias propiedades de activos		time-series		
BatchPutAssetPropertyValue	Concede permiso para poner valores de propiedad para propiedades de activos	Write	asset		
			time-series		
CreateAccessPolicy	Concede permiso para crear una política de acceso para un portal o un proyecto especificados	Write	portal		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	Concede permiso para crear un activo a partir de un modelo de activos	Write	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAssetModel	Concede permiso para crear una aplicación	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModelCompositeModel	Concede permiso para crear un modelo compuesto de modelo de activos dentro de un modelo de activos	Escritura	asset-model*		
CreateBulkImportJob	Concede permiso para crear un trabajo de importación masiva	Escritura			
CreateDashboard	Concede permiso para crear un panel en un proyecto	Escritura	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Concede permiso para crear un conjunto de datos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGateway	Concede permiso para crear una puerta de enlace	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortal	Concede permiso para crear un portal	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	Concede permiso para crear un proyecto en un portal	Write	portal*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPolicy	Concede permiso para eliminar una política de acceso	Write	access-policy*		
DeleteAsset	Concede permiso para eliminar un activo	Write	asset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAssetModel	Concede permiso para eliminar un modelo de activo	Escritura	asset-model*		
DeleteAssetModelCompositeModel	Concede permiso para eliminar un modelo compuesto de modelo de activos	Escritura	asset-model*		
DeleteDashboard	Concede permiso para eliminar un panel	Escritura	dashboard*		
DeleteDataset	Concede permiso para eliminar un conjunto de datos	Escritura	dataset*		
DeleteGateway	Concede permiso para eliminar una puerta de enlace	Write	gateway*		
DeletePortal	Concede permiso para eliminar un portal	Write	portal*		sso:DeleteManagedApplicationInstance
DeleteProject	Concede permiso para eliminar un proyecto	Escritura	project*		
DeleteTimeSeries	Concede permiso para eliminar una serie temporal	Escritura	asset		
			time-series		
DescribeAccessPolicy	Concede permiso para describir una política de acceso	Lectura	access-policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAction	Concede permiso para describir acciones	Lectura	asset		
DescribeAsset	Concede permiso para describir un activo	Lectura	asset*		
DescribeAssetCompositeModel	Concede permiso para describir modelo compuesto de activos	Lectura	asset*		
DescribeAssetModel	Concede permiso para describir modelo de activo	Lectura	asset-model*		
DescribeAssetModelCompositeModel	Concede permiso para describir modelo compuesto de modelo de activos	Lectura	asset-model*		
DescribeAssetProperty	Concede permiso para describir una propiedad de un activo	Lectura	asset*		
DescribeBulkImportJob	Concede permiso para describir un trabajo de importación masiva	Lectura			
DescribeDashboard	Concede permiso para describir un panel	Lectura	dashboard*		
DescribeDataset	Otorga permiso para describir el conjunto de datos	Lectura	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDefaultEncryptionConfiguration	Otorga permiso para describir la configuración de cifrado predeterminada para Cuenta de AWS	Lectura			
DescribeGateway	Concede permiso para describir una puerta de enlace	Read	gateway*		
DescribeGatewayCapabilityConfiguration	Concede permiso para describir una configuración de capacidad para una puerta de enlace	Lectura	gateway*		
DescribeLoggingOptions	Otorga permiso para describir las opciones de registro para Cuenta de AWS	Lectura			
DescribePortal	Concede permiso para describir un portal	Read	portal*		
DescribeProject	Concede permiso para describir un proyecto	Lectura	project*		
DescribeStorageConfiguration	Otorga permiso para describir la configuración de almacenamiento del Cuenta de AWS	Lectura			
DescribeTimeSeries	Concede permiso para describir una serie temporal	Lectura	asset time-series		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DisassociateAssets	Concede permiso para desasociar un activo secundario de un activo principal mediante una jerarquía	Escritura	asset*		
DisassociateTimeSeriesFromAssetProperty	Concede permiso para desvincular una serie temporal de una propiedad de activo	Escritura	asset* time-series*		
EnableSiteWiseIntegration [solo permiso]	Concede permiso para permitir que el IoT se SiteWise integre con otros servicios	Escritura			
ExecuteAction	Concede permiso para ejecutar acciones	Escritura	asset		
ExecuteQuery	Otorga permiso para ejecutar una consulta	Lectura			
GetAssetPropertyAggregates	Concede permiso para recuperar agregados calculados para una propiedad de activo	Read	asset time-series		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAssetPropertyValue	Concede permiso para recuperar el valor más reciente de una propiedad de activo	Read	asset		
			time-series		
GetAssetPropertyValueHistory	Concede permiso para recuperar el historial de valores de una propiedad de activo	Lectura	asset		
			time-series		
GetInterpolatedAssetPropertyValues	Concede permiso para recuperar valores interpolados de una propiedad de activo	Lectura	asset		
			time-series		
InvokeAssistant	Otorga permiso para invocar a un asistente	Lectura			
ListAccessPolicies	Concede permiso para enumerar todas las directivas de acceso para una identidad o un recurso	Enumeración	portal		
			project		
ListActions	Concede permiso para enumerar todas las acciones	Enumeración	asset		
ListAssetModelCompositeModels	Concede permiso para enumerar todos los modelos de activos	Enumeración	asset-model*		
ListAssetModelProperties	Otorga permiso para enumerar propiedades de modelos de activos	Enumeración	asset-model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssetModels	Concede permiso para enumerar todos los modelos de activos	Enumeración			
ListAssetProperties	Otorga permiso para enumerar las propiedades de los activos	Enumeración	asset*		
ListAssetRelationships	Concede permiso para enumerar el gráfico de relaciones de activos de un activo.	List	asset*		
ListAssets	Concede permiso para enumerar todos los activos	Enumeración	asset-model		
ListAssociatedAssets	Concede permiso para enumerar todos los activos asociados a un activo a través de una jerarquía	Enumeración	asset*		
ListBulkImportJobs	Concede permiso para enumerar trabajos de importación masiva	Enumeración			
ListCompositionRelationships	Concede permiso para enumerar todas las relaciones de composición del modelo de activos	Enumeración	asset-model*		
ListDashboards	Concede permiso para enumerar todos los paneles de un proyecto	Enumeración	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDatasets	Concede permiso para enumerar todos los conjuntos de datos	Enumeración			
ListGateways	Concede permiso para enumerar todas las puertas de enlace	List			
ListPortals	Concede permiso para enumerar todos los portales	List			
ListProjectAssets	Concede permiso para enumerar todos los activos asociados a un proyecto	List	project*		
ListProjects	Concede permiso para enumerar todos los proyectos en un portal	List	portal*		
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas para un recurso	Lectura	access-policy		
			asset		
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			project		
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	Concede permiso para enumerar series temporales	Enumeración	asset		
PutDefaultEncryptionConfiguration	Otorga permiso para establecer la configuración de cifrado predeterminada para Cuenta de AWS	Escritura			
PutLoggingOptions	Otorga permiso para configurar las opciones de registro para el Cuenta de AWS	Escritura			
PutStorageConfiguration	Otorga permiso para configurar los ajustes de almacenamiento para Cuenta de AWS	Escritura			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	access-policy		
			asset		
			asset-model		
			dashboard		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	access-policy		
			asset		
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	Concede permiso para actualizar una política de acceso	Write	access-policy*		
UpdateAsset	Concede permiso para actualizar un activo	Write	asset*		
UpdateAssetModel	Concede permiso para actualizar un modelo de activos	Escritura	asset-model*		
UpdateAssetModelCompositeModel	Concede permiso para actualizar un modelo compuesto de modelo de activos	Escritura	asset-model*		
UpdateAssetModelPropertyRouting [solo permiso]	Otorga permiso para actualizar el enrutamiento AssetModel de una propiedad	Escritura	asset-model*		
UpdateAssetProperty	Concede permiso para actualizar una propiedad de activo	Write	asset*		
UpdateDashboard	Concede permiso para actualizar un panel	Escritura	dashboard*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDataset	Concede permiso para actualizar un conjunto de datos	Escritura	dataset*		
UpdateGateway	Concede permiso para actualizar una puerta de enlace	Write	gateway*		
UpdateGatewayCapabilityConfiguration	Concede permiso para actualizar una configuración de capacidades para una puerta de enlace	Write	gateway*		
UpdatePortal	Concede permiso para actualizar un portal	Write	portal*		
UpdateProject	Concede permiso para actualizar un proyecto	Escritura	project*		

Tipos de recursos definidos por el AWS IoT SiteWise

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
asset	arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}	aws:ResourceTag/${TagKey}
asset-model	arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}	aws:ResourceTag/${TagKey}
time-series	arn:${Partition}:iotsitewise:${Region}:${Account}:time-series/${TimeSeriesId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}	aws:ResourceTag/${TagKey}
access-policy	arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:iotsitewise:${Region}:${Account}:dataset/${DatasetId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS IoT SiteWise

AWS El IoT SiteWise define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las

que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso	Cadena
aws:TagKeys	Filtra las acciones mediante las claves de etiqueta en la solicitud.	ArrayOfString
iotsitewise:assetHierarchyPath	Filtra el acceso mediante una ruta jerárquica de activos, que es la cadena de activos IDs en la jerarquía del activo, cada uno separado por una barra diagonal	Cadena
iotsitewise:childAssetId	Filtra el acceso mediante el ID de un activo secundario asociado a un activo principal.	Cadena
iotsitewise:group	Filtra el acceso por el ID de un grupo de inicio de sesión AWS único	Cadena
iotsitewise:iam	Filtra el acceso por el ID de una AWS identidad de IAM	Cadena
iotsitewise:isAssociatedWithAssetProperty	Filtra el acceso mediante secuencias de datos asociados o no asociados a las propiedades de activo.	Cadena
iotsitewise:portal	Filtra el acceso por ID de un portal	Cadena

Claves de condición	Descripción	Tipo
iotsitewise:project	Filtra el acceso por el ID de un proyecto	Cadena
iotsitewise:propertyAlias	Filtra el acceso mediante el alias de la propiedad.	Cadena
iotsitewise:propertyId	Filtra el acceso por el ID de una propiedad de activo	Cadena
iotsitewise:user	Filtra el acceso por el ID de un usuario de AWS Single Sign-On	Cadena

Claves de condiciones, recursos y acciones para el AWS IoT TwinMaker

AWS IoT TwinMaker (prefijo de servicio:`iottwinmaker`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el AWS IoT TwinMaker
- Tipos de recursos definidos por el AWS IoT TwinMaker
- Claves de condición para AWS IoT TwinMaker

Acciones definidas por el AWS IoT TwinMaker

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchPutPropertyValues	Otorga permiso para establecer valores para varias propiedades de series temporales.	Escritura	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		
CancelMetadataTransferJob	Concede permiso para cancelar un trabajo de transferencia de metadatos	Escritura	metadataTransferJob*		
CreateComponentType	Otorga permiso para crear un componentType.	Escritura	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEntity	Otorga permiso para crear una entidad.	Escritura	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	Concede permiso para crear un trabajo de transferencia de metadatos	Escritura			
CreateScene	Otorga permiso para crear una escena.	Escritura	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	Otorga permiso para crear un trabajo de sincronización	Escritura	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateWorkspace	Concede permiso para crear un espacio de trabajo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	Otorga permiso para eliminar un componentType.	Escritura	componentType* workspace*		
DeleteEntity	Otorga permiso para eliminar una entidad.	Escritura	entity* workspace*		
DeleteScene	Otorga permiso para eliminar una escena.	Escritura	scene* workspace*		
DeleteSyncJob	Otorga permiso para eliminar un trabajo. de sincronización	Escritura	syncJob* workspace*		
DeleteWorkspace	Concede permiso para eliminar un espacio de trabajo	Escritura	workspace*		
ExecuteQuery	Otorga permiso para ejecutar una consulta	Lectura	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetComponentType	Otorga permiso para obtener un componentType	Lectura	componentType*		
			workspace*		
GetEntity	Otorga permiso para obtener una entidad.	Lectura	entity*		
			workspace*		
GetMetadataTransferJob	Concede permiso para obtener trabajo de transferencia de metadatos	Lectura	metadataTransferJob*		
GetPricingPlan	Otorga permiso para obtener un plan de precios	Lectura			
GetPropertyValue	Otorga permiso para recuperar los valor de una propiedad.	Lectura	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			entity		
GetPropertyValueHistory	Otorga permiso para recuperar el historial de valores de una serie temporal.	Lectura	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetScene	Otorga permiso para obtener una escena.	Lectura	scene*		
			workspace*		
GetSyncJob	Otorga permiso para obtener un trabajo de sincronización	Lectura	syncJob*		
			workspace*		
GetWorkspace	Otorga permiso para obtener un área de trabajo.	Lectura	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListComponentTypes	Otorga permiso para enumerar todos los componentTypes de un área de trabajo.	Enumeración	workspace*		
ListComponents	Concede permiso para enumerar los componentes adjuntados a una entidad	Enumeración	entity* workspace*		
ListEntities	Otorga permiso para enumerar todas las entidades de un área de trabajo.	Enumeración	workspace*		
ListMetadataTransferJobs	Concede permiso para enumerar todos los trabajos de transferencia de metadatos	Enumeración			
ListProperties	Concede permiso para enumerar las propiedades de un componente de entidad	Enumeración	entity* workspace*		
ListScenes	Otorga permiso para enumerar todas las escenas de un área de trabajo.	Enumeración	workspace*		
ListSyncJobs	Otorga permiso para enumerar todos los trabajos de sincronización en un área de trabajo	Enumeración	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSyncResources	Otorga permiso para enumerar todos los recursos de sincronización de una tarea de sincronización	Enumeración	syncJob*		
			workspace*		
ListTagsForResource	Concede permiso para enumerar todas las etiquetas de un recurso	Enumeración	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:ResourceTag/${TagKey}	
ListWorkspaces	Otorga permiso para enumerar todas las áreas de trabajo.	Enumeración			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	componentType		
			entity		
			scene		
			syncJob		
			workspace		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:TagKeys	
UpdateComponentType	Otorga permiso para actualizar un componentType.	Escritura	componentType*		
			workspace*		
UpdateEntity	Otorga permiso para actualizar una entidad.	Escritura	entity*		
			workspace*		
UpdatePricingPlan	Otorga permiso para actualizar un plan de precios	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateScene	Da permiso para actualizar un una escena.	Escritura	scene*		
			workspace*		
UpdateWorkspace	Otorga permiso para actualizar un área de trabajo.	Escritura	workspace*		

Tipos de recursos definidos por el AWS IoT TwinMaker

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
workspace	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}`	aws:ResourceTag/${TagKey}
entity	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/entity/${EntityId}`	aws:ResourceTag/${TagKey}
componentType	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/component-type/${ComponentTypeId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
scene	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/scene/${SceneId}`	aws:ResourceTag/${TagKey}
syncJob	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/sync-job/${SyncJobId}`	aws:ResourceTag/${TagKey}
metadataTransferJob	`arn:${Partition}:iottwinmaker:${Region}:${Account}:metadata-transfer-job/${MetadataTransferJobId}`	

Claves de condición para AWS IoT TwinMaker

AWS El IoT TwinMaker define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso	Cadena
aws:TagKeys	Filtra las acciones mediante las claves de etiqueta en la solicitud.	ArrayOfString

Claves de condición	Descripción	Tipo
iottwinmaker:destinationType	Filtra el acceso por tipo de destino del trabajo de transferencia de metadatos	ArrayOfString
iottwinmaker:linkedServices	Filtra el acceso por espacio de trabajo vinculado a los servicios	ArrayOfString
iottwinmaker:sourceType	Filtra el acceso por tipo de fuente del trabajo de transferencia de metadatos	ArrayOfString

Acciones, recursos y claves de condición para AWS IoT Wireless

AWS IoT Wireless (prefijo de servicio:`iotwireless`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IoT Wireless
- Tipos de recurso definidos por AWS IoT Wireless
- Claves de condición de AWS IoT Wireless

Acciones definidas por AWS IoT Wireless

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateAwsAccountWithPartnerAccount	Otorga permiso para vincular las cuentas de los socios con Cuenta de AWS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateMulticastGroupWithFuotaTask	Otorga permiso para asociarlo MulticastGroup con FuotaTask	Escritura	FuotaTask* MulticastGroup*		
AssociateWirelessDeviceWithFuotaTask	Otorga permiso para asociar el dispositivo inalámbrico con FuotaTask	Escritura	FuotaTask* WirelessDevice*		
AssociateWirelessDeviceWithMulticastGroup	Otorga permiso para asociar el WirelessDevice con MulticastGroup	Escritura	MulticastGroup* WirelessDevice*		
AssociateWirelessDeviceWithThing	Otorga permiso para asociar el dispositivo inalámbrico con el AWS IoT por un momento dado wirelessDeviceId	Escritura	WirelessDevice* thing*		iot:DescribeThing
AssociateWirelessG	Otorga permiso para asociar a WirelessGateway con el certificado IoT Core Identity	Escritura	WirelessGateway* cert*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
atewayWithCertificate					
AssociateWirelessGatewayWithThing	Otorga permiso para asociar la puerta de enlace inalámbrica con el AWS IoT por un momento dado wirelessGatewayId	Escritura	WirelessGateway* thing*		iot:DescribeThing
CancelMulticastGroupSession	Otorga permiso para cancelar la MulticastGroup sesión	Escritura	MulticastGroup*		
CreateDestination	Otorga permiso para crear un recurso Destination	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceProfile	Otorga permiso para crear un DeviceProfile recurso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFuotaTask	Otorga permiso para crear un FuotaTask recurso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMulticastGroup	Otorga permiso para crear un MulticastGroup recurso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkAnalyzerConfiguration	Otorga permiso para crear un NetworkAnalyzerConfiguration recurso	Escritura	MulticastGroup*		
			WirelessDevice*		
			WirelessGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceProfile	Otorga permiso para crear un ServiceProfile recurso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateWirelessDevice	Otorga permiso para crear un WirelessDevice recurso con un destino determinado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGateway	Otorga permiso para crear un WirelessGateway recurso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGatewayTask	Otorga permiso para crear una tarea para una determinada WirelessGateway	Escritura	WirelessGateway*		
CreateWirelessGatewayTaskDefinition	Otorga permiso para crear una definición de WirelessGateway tarea	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDestination	Otorga permiso para eliminar un Destination	Escritura	Destination*		
DeleteDeviceProfile	Otorga permiso para eliminar una DeviceProfile	Escritura	DeviceProfile*		
DeleteFuotaTask	Otorga permiso para eliminar el FuotaTask	Escritura	FuotaTask*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMulticastGroup	Otorga permiso para eliminar el MulticastGroup	Escritura	MulticastGroup*		
DeleteNetworkAnalyzerConfiguration	Otorga permiso para eliminar el NetworkAnalyzerConfiguration	Escritura	NetworkAnalyzerConfiguration*		
DeleteQueuedMessages	Otorga permiso para eliminar QueuedMessages	Escritura			
DeleteServiceProfile	Otorga permiso para eliminar un ServiceProfile	Escritura	ServiceProfile*		
DeleteWirelessDevice	Otorga permiso para eliminar un WirelessDevice	Escritura	WirelessDevice*		
DeleteWirelessDeviceImportTask	Concede permiso para eliminar la tarea de importación de dispositivos inalámbricos	Escritura	ImportTask*		
DeleteWirelessGateway	Otorga permiso para eliminar un WirelessGateway	Escritura	WirelessGateway*		
DeleteWirelessGatewayTask	Otorga permiso para eliminar una tarea determinada WirelessGateway	Escritura	WirelessGateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteWirelessGatewayTaskDefinition	Otorga permiso para eliminar una definición de WirelessGateway tarea	Escritura	WirelessGatewayTaskDefinition*		
DeregisterWirelessDevice	Concede permiso para anular el registro de un dispositivo inalámbrico	Escritura	WirelessDevice*		
DisassociateAwsAccountFromPartnerAccount	Otorga permiso para desasociar una Cuenta de AWS cuenta asociada	Escritura	SidewalkAccount*		
DisassociateMulticastGroupFromFuotaTask	Otorga permiso para desvincular la de MulticastGroup FuotaTask	Escritura	FuotaTask*		
			MulticastGroup*		
DisassociateWirelessDeviceFromFuotaTask	Otorga permiso para desvincular el dispositivo inalámbrico de FuotaTask	Escritura	FuotaTask*		
			WirelessDevice*		
DisassociateWirelessDeviceFromMulticastGroup	Otorga permiso para desvincular el dispositivo inalámbrico de MulticastGroup	Escritura	MulticastGroup*		
			WirelessDevice*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateWirelessDeviceFromThing	Otorga permiso para desasociar un dispositivo inalámbrico de una cosa de AWS IoT	Escritura	WirelessDevice*		iot:DescribeThing
			thing*		
DisassociateWirelessGatewayFromCertificate	Otorga permiso para desasociar a WirelessGateway de un certificado de identidad central de IoT	Escritura	WirelessGateway*		
			cert*		
DisassociateWirelessGatewayFromThing	Otorga permiso para desasociar una WirelessGateway cosa de la IoT Core	Escritura	WirelessGateway*		iot:DescribeThing
			thing*		
GetDestination	Otorga permiso para obtener el Destination	Lectura	Destination*		
GetDeviceProfile	Otorga permiso para obtener el DeviceProfile	Lectura	DeviceProfile*		
GetEventConfigurationByResourceTypes	Otorga permiso para obtener configuraciones de eventos según los tipos de recursos	Lectura			
GetFuotaTask	Otorga permiso para obtener el FuotaTask	Lectura	FuotaTask*		
GetLogLevelsByResourceTypes	Otorga permiso para obtener niveles de registro por tipos de recursos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMetricConfiguration	Concede permiso para obtener la configuración de métricas	Lectura			
GetMetrics	Concede permiso para obtener métricas	Lectura			
GetMulticastGroup	Otorga permiso para obtener el MulticastGroup	Lectura	MulticastGroup*		
GetMulticastGroupSession	Otorga permiso para obtener la MulticastGroup sesión	Lectura	MulticastGroup*		
GetNetworkAnalyzerConfiguration	Otorga permiso para obtener el NetworkAnalyzerConfiguration	Lectura	NetworkAnalyzerConfiguration*		
GetPartnerAccount	Otorga permiso para obtener el asociado PartnerAccount	Lectura	SidewalkAccount*		
GetPosition	Otorga permiso para mostrar una lista de etiquetas de un recurso determinado.	Lectura	WirelessDevice		
			WirelessGateway		
GetPositionConfiguration	Otorga permiso para obtener la configuración de la posición de un recurso determinado.	Lectura	WirelessDevice		
			WirelessGateway		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPositionEstimate	Otorga permiso para obtener una estimación de la posición	Lectura			
GetResourceEventConfiguration	Otorga permiso para obtener una configuración de evento para un identificador.	Lectura	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
GetResourceLogLevel	Otorga permiso para obtener niveles de registro de recursos.	Lectura	WirelessDevice		
			WirelessGateway		
GetResourcePosition	Otorga permiso para mostrar una lista de etiquetas de un recurso determinado.	Lectura	WirelessDevice		
			WirelessGateway		
GetServiceEndpoint	Otorga permiso para recuperar el punto final específico de la cuenta del cliente para la conexión con el protocolo CUPS o la conexión con el protocolo del servidor de red LoRa WAN (LNS) y, opcionalmente, el certificado de confianza del servidor en formato PEM	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceProfile	Otorga permiso para obtener el ServiceProfile	Lectura	ServiceProfile*		
GetWirelessDevice	Otorga permiso para obtener el WirelessDevice	Lectura	WirelessDevice*		
GetWirelessDeviceImportTask	Concede permiso para obtener la tarea de importación de dispositivos inalámbricos	Lectura	ImportTask*		
GetWirelessDeviceStatistics	Otorga permiso para obtener información estadística sobre una determinada WirelessDevice	Lectura	WirelessDevice*		
GetWirelessGateway	Otorga permiso para obtener el WirelessGateway	Lectura	WirelessGateway*		
GetWirelessGatewayCertificate	Otorga permiso para obtener el identificador del certificado de IoT Core Identity asociado al WirelessGateway	Lectura	WirelessGateway*		
GetWirelessGatewayFirmwareInformation	Otorga permiso para obtener la versión actual del firmware y otra información para WirelessGateway	Lectura	WirelessGateway*		
GetWirelessGatewayStatistics	Otorga permiso para obtener información estadística sobre una determinada WirelessGateway	Lectura	WirelessGateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetWirelessGatewayTask	Otorga permiso para obtener la tarea de una determinada WirelessGateway	Lectura	WirelessGateway*		
GetWirelessGatewayTaskDefinition	Otorga permiso para obtener la definición de WirelessGateway tarea dada	Lectura	WirelessGatewayTaskDefinition*		
ListDestinations	Otorga permiso para incluir información sobre los destinos disponibles en función de Cuenta de AWS	Lectura			
ListDeviceProfiles	Otorga permiso para incluir la información disponible en DeviceProfiles función de Cuenta de AWS	Lectura			
ListDevicesForWirelessDeviceImportTask	Otorga permiso para enumerar la información de los dispositivos por tarea de importación de dispositivos inalámbricos en función de Cuenta de AWS	Lectura	ImportTask*		
ListEventConfigurations	Otorga permiso para incluir información sobre las configuraciones de eventos disponibles en función de Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFuotaTasks	Otorga permiso para enumerar la información disponible en FuotaTasks función de Cuenta de AWS	Lectura			
ListMulticastGroups	Otorga permiso para incluir la información disponible en MulticastGroups función de Cuenta de AWS	Lectura			
ListMulticastGroupsByFuotaTask	Otorga permiso para enumerar la información disponible MulticastGroups en FuotaTask función de Cuenta de AWS	Lectura	FuotaTask *		
ListNetworkAnalyzerConfigurations	Otorga permiso para enumerar la información disponible en NetworkAnalyzerConfigurations función de Cuenta de AWS	Lectura			
ListPartnerAccounts	Otorga permiso para mostrar las cuentas de socio disponibles	Lectura			
ListPositionConfigurations	Otorga permiso para incluir información sobre las configuraciones de posición disponibles en función de Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQueuedMessages	Otorga permiso para mostrar los mensajes en cola	Lectura			
ListServiceProfiles	Otorga permiso para incluir la información disponible en ServiceProfiles función de Cuenta de AWS	Lectura			
ListTagsForResource	Concede permiso para mostrar todas las etiquetas de un recurso determinado	Lectura	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			WirelessGateway		
			WirelessGatewayTaskDefinition		
ListWirelessDeviceImportTasks	Otorga permiso para enumerar la información de las tareas de importación de dispositivos inalámbricos en función de Cuenta de AWS	Lectura			
ListWirelessDevices	Otorga permiso para enumerar la información disponible en WirelessDevices función de Cuenta de AWS	Lectura			
ListWirelessGatewayTaskDefinitions	Otorga permiso para incluir información sobre las definiciones de WirelessGateway tareas disponibles en función de Cuenta de AWS	Lectura			
ListWirelessGateways	Otorga permiso para enumerar la información disponible en WirelessGateways función de Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutPositionConfiguration	Otorga permiso para configurar la posición de un recurso determinado.	Escritura	WirelessDevice		
			WirelessGateway		
PutResourceLogLevel	Otorga permiso para colocar niveles de registro de recursos.	Write	WirelessDevice		
			WirelessGateway		
ResetAllResourceLogLevels	Otorga permiso para restablecer todos los niveles de registro de recursos.	Write			
ResetResourceLogLevel	Otorga permiso para restablecer un nivel de registro de recursos.	Escritura	WirelessDevice		
			WirelessGateway		
SendDataToMulticastGroup	Otorga permiso para enviar datos al MulticastGroup	Escritura	MulticastGroup*		
SendDataToWirelessDevice	Otorga permiso para enviar la trama de datos de la aplicación descifrada al dispositivo de destino	Escritura	WirelessDevice*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartBulkAssociateWirelessDeviceWithMulticastGroup	Otorga permiso para asociarlo WirelessDevices con Multicast Group	Escritura	MulticastGroup*		
StartBulkDisassociateWirelessDeviceFromMulticastGroup	Otorga permiso para desasociar de forma masiva el WirelessDevices Multicast Group	Escritura	MulticastGroup*		
StartFuotaTask	Otorga permiso para iniciar el FuotaTask	Escritura	FuotaTask*		
StartMulticastGroupSession	Otorga permiso para iniciar la MulticastGroup sesión	Escritura	MulticastGroup*		
StartNetworkAnalyzerStream	Otorga permiso para iniciar la NetworkAnalyzer transmisión	Escritura	NetworkAnalyzerConfiguration*		
StartSingleWirelessDeviceImportTask	Concede permiso para iniciar la tarea de importación de un dispositivo inalámbrico único	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartWirelessDeviceImportTask	Concede permiso para iniciar la tarea de importación de dispositivos inalámbricos	Escritura	ImportTask*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Otorga permiso para etiquetar un recurso determinado	Etiquetado	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestWirelessDevice	Otorga permiso para simular un dispositivo aprovisionado a fin de enviar datos de enlace ascendente con carga de "Hola"	Write	WirelessDevice*		
UntagResource	Otorga permiso para quitar las etiquetas determinadas del recurso	Etiquetado	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Multicast Group		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:TagKeys	
UpdateDestination	Otorga permiso para actualizar un recurso Destination	Escritura	Destination*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEventConfigurationByResourceTypes	Otorga permiso para actualizar configuraciones de evento según los tipos de recursos	Escritura			
UpdateFuotaTask	Otorga permiso para actualizar el FuotaTask	Escritura	FuotaTask*		
UpdateLogLevelsByResourceTypes	Otorga permiso para actualizar niveles de registro por tipos de recursos	Escritura			
UpdateMetricConfiguration	Concede permiso para actualizar la configuración de métricas	Escritura			
UpdateMulticastGroup	Otorga permiso para actualizar el MulticastGroup	Escritura	MulticastGroup*		
UpdateNetworkAnalyzerConfiguration	Otorga permiso para actualizar el NetworkAnalyzerConfiguration	Escritura	MulticastGroup*		
			NetworkAnalyzerConfiguration*		
			WirelessDevice*		
			WirelessGateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePartnerAccount	Otorga permiso para actualizar una cuenta de socio	Escritura	SidewalkAccount*		
UpdatePosition	Otorga permiso para actualizar la posición de un recurso determinado.	Escritura	WirelessDevice		
			WirelessGateway		
UpdateResourceEventConfiguration	Otorga permiso para actualizar una configuración de eventos para un identificador.	Escritura	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
UpdateResourcePosition	Otorga permiso para actualizar la posición de un recurso determinado.	Escritura	WirelessDevice		
			WirelessGateway		
UpdateWirelessDevice	Otorga permiso para actualizar un WirelessDevice recurso	Escritura	WirelessDevice*		
UpdateWirelessDeviceImportTask	Concede permiso para actualizar una tarea de importación de dispositivos inalámbricos	Escritura	ImportTask*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateWirelessGateway	Otorga permiso para actualizar un WirelessGateway recurso	Escritura	WirelessGateway*		

Tipos de recurso definidos por AWS IoT Wireless

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
WirelessDevice	`arn:${Partition}:iotwireless:${Region}:${Account}:WirelessDevice/${WirelessDeviceId}`	aws:ResourceTag/${TagKey}
WirelessGateway	`arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGateway/${WirelessGatewayId}`	aws:ResourceTag/${TagKey}
DeviceProfile	`arn:${Partition}:iotwireless:${Region}:${Account}:DeviceProfile/${DeviceProfileId}`	aws:ResourceTag/${TagKey}
ServiceProfile	`arn:${Partition}:iotwireless:${Region}:${Account}:ServiceProfile/${ServiceProfileId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Destination	arn:${Partition}:iotwireless:${Region}:${Account}:Destination/${DestinationName}	aws:ResourceTag/${TagKey}
SidewalkAccount	arn:${Partition}:iotwireless:${Region}:${Account}:SidewalkAccount/${SidewalkAccountId}	aws:ResourceTag/${TagKey}
WirelessGatewayTaskDefinition	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGatewayTaskDefinition/${WirelessGatewayTaskDefinitionId}	aws:ResourceTag/${TagKey}
FuotaTask	arn:${Partition}:iotwireless:${Region}:${Account}:FuotaTask/${FuotaTaskId}	aws:ResourceTag/${TagKey}
MulticastGroup	arn:${Partition}:iotwireless:${Region}:${Account}:MulticastGroup/${MulticastGroupId}	aws:ResourceTag/${TagKey}
NetworkAnalyzerConfiguration	arn:${Partition}:iotwireless:${Region}:${Account}:NetworkAnalyzerConfiguration/${NetworkAnalyzerConfigurationName}	aws:ResourceTag/${TagKey}
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
cert	arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}	
ImportTask	arn:${Partition}:iotwireless:${Region}:${Account}:ImportTask/${ImportTaskId}	aws:ResourceTag/${TagKey}

Claves de condición de AWS IoT Wireless

AWS IoT Wireless define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta presente en la solicitud que el usuario realiza a IoT Wireless	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por componente clave de etiqueta de una etiqueta asociada a un recurso de IoT Wireless	Cadena
aws:TagKeys	Filtra el acceso en función de la lista de todos los nombres de clave de etiqueta asociados con el recurso en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS IQ

AWS IQ (prefijo de servicio:`iq`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IQ
- Tipos de recursos definidos por AWS IQ
- Claves de condición para AWS IQ

Acciones definidas por AWS IQ

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptCall	Otorga permiso para aceptar una llamada entrante voice/video	Escritura	call*		
ApprovePaymentRequest	Otorga permiso para aprobar una solicitud de pago	Escritura	paymentRequest*		
ApproveProposal	Otorga permiso para aprobar una propuesta	Escritura	proposal*		
ArchiveConversation	Otorga permiso para archivar una conversación	Escritura	conversation*		
CompleteProposal	Otorga permiso para completar una propuesta	Escritura	proposal*		
CreateConversation	Otorga permiso para responder a una solicitud o enviar un mensaje directo para iniciar una conversación	Escritura			
CreateExpert	Otorga permiso para crear un perfil experto	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateListing	Otorga permiso para crear una lista	Escritura			
CreateMilestoneProposal	Otorga permiso para crear una propuesta de hito	Escritura			
CreatePaymentRequest	Otorga permiso para crear una solicitud de pago	Escritura			
CreateProject	Otorga permiso para enviar nuevas solicitudes	Escritura			
CreateRequest	Otorga permiso para enviar nuevas solicitudes	Escritura			
CreateScheduledProposal	Otorga permiso para crear una propuesta programada	Escritura			
CreateSeller	Otorga permiso para crear un perfil de vendedor	Escritura			
CreateUpfrontProposal	Otorga permiso para crear una propuesta inicial	Escritura			
DeclineCall	Otorga permiso para rechazar una voice/video llamada entrante	Escritura	call*		
DeleteAttachment	Otorga permiso para eliminar un adjunto existente	Escritura	attachment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableIndividualPublicProfile	Concede permiso para desactivar la página de perfil público individual	Escritura	expert*		
DownloadAttachment	Concede permiso para descargar un adjunto existente	Lectura	attachment*		
EnableIndividualPublicProfile	Concede permiso para habilitar la página de perfil público individual	Escritura	expert*		
EndCall	Otorga permiso para finalizar una voice/video llamada	Escritura	call*		
GetBuyer	Otorga permiso para leer la información del comprador	Lectura	buyer*		
GetCall	Otorga permiso para leer los detalles de una voice/video llamada	Lectura	call*		
GetChatInfo	Otorga permiso para leer detalles del entorno de chat acerca de una conversación	Lectura	conversation*		
GetChatMessages	Otorga permiso para leer mensajes de chat en una conversación	Lectura	conversation*		
GetChatToken	Otorga permiso para solicitar un token de websocket para las notificaciones de conversación	Lectura	token*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCompanyChatMessages	Concede permiso para leer mensajes de chat en una conversación de la compañía	Lectura	conversation*		
GetCompanyProfile	Otorga permiso para leer el perfil de una empresa	Lectura	company*		
GetConversation	Otorga permiso para leer detalles de una conversación	Lectura	conversation*		
GetExpert	Otorga permiso para leer la información experta	Lectura	expert*		
GetListing	Otorga permiso para leer una lista	Lectura	listing*		
GetMarketplaceSeller	Otorga permiso para leer la información del perfil de un vendedor	Lectura	seller*		
GetPaymentRequest	Otorga permiso para leer una solicitud de pago	Lectura	paymentRequest*		
GetProposal	Otorga permiso para leer una propuesta	Lectura	proposal*		
GetRequest	Concede permiso para obtener una solicitud creada	Lectura	request*		
GetReview	Otorga permiso para leer una reseña para un experto	Lectura	seller*		
HideRequest	Otorga permiso para ocultar una solicitud.	Escritura	request*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InitiateCall	Otorga permiso para iniciar una voice/video llamada	Escritura			
LinkAwsCertification	Otorga permiso para vincular una AWS certificación a un perfil individual	Escritura	expert*		
ListAttachments	Concede permiso para enumerar los adjuntos existentes	Enumeración	attachment*		
ListConversations	Otorga permiso para enumerar las conversiones existentes	Lectura	conversation*		
ListExpertAccessLogs	Concede permiso para enumerar los registros de acceso de la actividad de los expertos	Lectura	permission*		
ListListings	Otorga permiso para enumerar las listas	Lectura	listing*		
ListPaymentRequests	Otorga permiso para enumerar las solicitudes de pago	Lectura	paymentRequest		
			paymentSchedule		
ListProposals	Otorga permiso para enumerar propuestas	Lectura	proposal*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRequests	Otorga permiso para enumerar las solicitudes que se crean	Lectura	request*		
ListReviews	Otorga permiso para enumerar las revisiones para un experto	Lectura	seller*		
MarkChatMessageRead	Otorga permiso para marcar un mensaje como leído en una conversación	Escritura	conversation*		
RejectPaymentRequest	Otorga permiso para rechazar la solicitud de pagos	Escritura	paymentRequest*		
RejectProposal	Otorga permiso para rechazar una propuesta	Escritura	proposal*		
SendCompanyChatMessage	Otorga permiso para enviar un mensaje en una conversación como empresa	Escritura	conversation*		
SendIndividualChatMessage	Otorga permiso para enviar un mensaje en una conversación de forma individual	Escritura	conversation*		
UnarchiveConversation	Otorga permiso para desarchivar una conversación	Escritura	conversation*		
UnlinkAwsCertification	Otorga permiso para desvincular una AWS certificación del perfil individual	Escritura	expert*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCompanyProfile	Otorga permiso para actualizar el perfil de una compañía	Escritura	company*		
UpdateConversationMembers	Otorga permiso para añadir más participantes a una conversación	Escritura	conversation*		
UpdateExpert	Otorga permiso para actualizar información de un experto	Escritura	expert*		
UpdateListing	Otorga permiso para actualizar una lista	Escritura	listing*		
UpdateRequest	Otorga permiso para actualizar una solicitud	Escritura	request*		
UploadAttachment	Otorga permiso para cargar un adjunto	Escritura			
WithdrawPaymentRequest	Otorga permiso para retirar una solicitud de pago	Escritura	paymentRequest*		
WithdrawProposal	Otorga permiso para retirar una propuesta	Escritura	proposal*		
WriteReview	Otorga permiso para escribir una reseña para un experto	Escritura	seller*		

Tipos de recursos definidos por AWS IQ

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
conversation	`arn:${Partition}:iq:${Region}::conversation/${ConversationId}`	
buyer	`arn:${Partition}:iq:${Region}::buyer/${BuyerId}`	
expert	`arn:${Partition}:iq:${Region}::expert/${ExpertId}`	
call	`arn:${Partition}:iq:${Region}::call/${CallId}`	
token	`arn:${Partition}:iq:${Region}::token/${TokenId}`	
proposal	`arn:${Partition}:iq:${Region}::proposal/${ConversationId}/${ProposalId}`	
paymentRequest	`arn:${Partition}:iq:${Region}::paymentRequest/${ConversationId}/${ProposalId}/${PaymentRequestId}`	
paymentSchedule	`arn:${Partition}:iq:${Region}::paymentSchedule/${ConversationId}/${ProposalId}/${VersionId}`	
seller	`arn:${Partition}:iq:${Region}::seller/${SellerAwsAccountId}`	
company	`arn:${Partition}:iq:${Region}::company/${CompanyId}`	

Tipos de recurso	ARN	Claves de condición
request	`arn:${Partition}:iq:${Region}::request/${RequestId}`	
listing	`arn:${Partition}:iq:${Region}::listing/${ListingId}`	
attachment	`arn:${Partition}:iq:${Region}::attachment/${AttachmentId}`	
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Claves de condición para AWS IQ

IQ no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS IQ Permissions

AWS IQ Permissions (prefijo de servicio:`iq-permission`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS IQ Permissions

- Tipos de recursos definidos por AWS IQ Permissions
- Claves de condición para AWS IQ Permissions

Acciones definidas por AWS IQ Permissions

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApproveAccessGrant	Otorga permiso para aprobar una solicitud de permiso	Escritura	permission*		
ApprovePermissionRequest	Otorga permiso para aprobar una solicitud de permiso	Escritura	permission*		
AssumePermissionRole	Otorga permiso para obtener un conjunto de credenciales de seguridad temporales para que los expertos puedan utilizarlas para acceder a los recursos de los compradores AWS	Escritura	permission*		
CreatePermissionRequest	Otorga permiso para crear una solicitud de permiso	Escritura	permission*		
GetPermissionRequest	Otorga permiso para obtener una solicitud de permiso	Lectura	permission*		
ListPermissionRequests	Otorga permiso para enumerar solicitudes de permiso	Lectura	permission*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RejectPermissionRequest	Otorga permiso para rechazar una solicitud de permiso	Escritura	permission*		
RevokePermissionRequest	Otorga permiso para revocar una solicitud de permiso que se aprobó anteriormente	Escritura	permission*		
WithdrawPermissionRequest	Otorga permiso para retirar una solicitud de permiso que no ha sido aprobada o rechazada	Escritura	permission*		

Tipos de recursos definidos por AWS IQ Permissions

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Claves de condición para AWS IQ Permissions

IQ Permissions no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Kendra

Amazon Kendra (prefijo de servicio: `kendra`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicas del servicio para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kendra
- Tipos de recursos definidos por Amazon Kendra
- Claves de condición para Amazon Kendra

Acciones definidas por Amazon Kendra

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateEntitiesToExperience	Otorga permiso para colocar el mapeo de entidades principales en el índice	Escritura	experience*		
			index*		
AssociatePersonasToEntities	Define los permisos específicos de los usuarios o grupos en su fuente de identidad de AWS SSO con acceso a su experiencia de Amazon Kendra	Escritura	experience*		
			index*		
BatchDeleteDocument	Concede permiso para documento de eliminación por lotes	Escritura	index*		
BatchDeleteFeaturedResultsSet	Concede permiso para eliminar un conjunto de resultados destacados	Escritura	featured-results-set*		
			index*		
BatchGetDocumentStatus	Otorga permiso para obtener el estado del documento por lotes	Lectura	index*		
BatchPutDocument	Otorga permiso para documento de inserción por lotes	Escritura	index*		
ClearQuerySuggestions	Otorga permiso para borrar las sugerencias de un índice	Escritura	index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	determinado generadas hasta el momento				
CreateAccessControlConfiguration	Concede permiso para crear una configuración del control de acceso	Escritura	index*		
CreateDataSource	Concede permiso para crear un origen de datos	Escritura	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExperience	Crea una experiencia de Amazon Kendra, como una aplicación de búsqueda	Escritura	index*		
CreateFaq	Otorga permiso para crear una pregunta frecuente	Escritura	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeaturedResultsSet	Concede permiso para crear un conjunto de resultados destacados	Escritura	index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Otorga permiso para crear un índice	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuerySuggestionsBlockList	Otorga permiso para crear un QuerySuggestions BlockList	Escritura	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThesaurus	Otorga permiso para crear un diccionario	Escritura	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccessControlConfiguration	Concede permiso para eliminar una configuración del control de acceso	Escritura	access-control-configuration*		
			index*		
DeleteDataSource	Concede permiso para eliminar un origen de datos	Escritura	data-source*		
			index*		
DeleteExperience	Elimina la experiencia de Amazon Kendra, como una aplicación de búsqueda	Escritura	experience*		
			index*		
DeleteFaq	Otorga permiso para eliminar una pregunta frecuente	Escritura	faq*		
			index*		
DeleteIndex	Otorga permiso para eliminar un índice	Escritura	index*		
DeletePrincipalMapping	Otorga permiso para eliminar el mapeo principal del índice	Escritura	index*		
			data-source		
DeleteQuerySuggestionsBlockList	Otorga permiso para eliminar un QuerySuggestions BlockList	Escritura	index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			query-suggestions-block-list*		
DeleteThesaurus	Otorga permiso para eliminar un diccionario	Escritura	index*		
			thesaurus*		
DescribeAccessControlConfiguration	Concede permiso para describir una configuración del control de acceso	Lectura	access-control-configuration*		
			index*		
DescribeDataSource	Concede permiso para describir un origen de datos	Lectura	data-source*		
			index*		
DescribeExperience	Obtiene información sobre la experiencia de Amazon Kendra, como una aplicación de búsqueda	Lectura	experience*		
			index*		
DescribeFaq	Otorga permiso para describir una pregunta frecuente	Lectura	faq*		
			index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFeaturedResultsSet	Concede permiso para describir un conjunto de resultados destacados	Lectura	featured-results-set*		
			index*		
DescribeIndex	Otorga permiso para describir un índice	Lectura	index*		
DescribePrincipalMapping	Otorga permiso para describir el mapeo de entidades principales del índice	Lectura	index*		
			data-source		
DescribeQuerySuggestionsBlockList	Otorga permiso para describir un QuerySuggestions BlockList	Lectura	index*		
			query-suggestions-block-list*		
DescribeQuerySuggestionsConfig	Otorga permiso para describir la configuración de sugerencias de consulta para un índice	Lectura	index*		
DescribeThesaurus	Otorga permiso para describir un diccionario	Lectura	index*		
			thesaurus*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateEntitiesFromExperience	Impide que los usuarios o grupos de su fuente de identidad de AWS SSO accedan a su experiencia de Amazon Kendra	Escritura	experience*		
			index*		
DisassociatePersonasFromEntities	Elimina los permisos específicos de los usuarios o grupos de tu fuente de identidad de AWS SSO con acceso a tu experiencia con Amazon Kendra	Escritura	experience*		
			index*		
GetQuerySuggestions	Otorga permiso para obtener sugerencias para un prefijo de consulta	Lectura	index*		
GetSnapshots	Recupera los datos de las métricas de búsqueda	Lectura	index*		
ListAccessControlConfigurations	Concede permiso para enumerar la configuración del control de acceso	Enumeración	index*		
ListDataSourceSyncJobs	Concede permiso para obtener el historial de trabajos de sincronización de orígenes de datos	Enumeración	data-source*		
			index*		
ListDataSources	Otorga permiso para enumerar los orígenes de datos	Enumeración	index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntityPersonas	Muestra los permisos específicos de los usuarios y grupos con acceso a la experiencia de Amazon Kendra	Enumeración	experience*		
			index*		
ListExperienceEntities	Muestra los usuarios o grupos de su fuente de identidad de AWS SSO a los que se les ha concedido acceso a su experiencia de Amazon Kendra	Enumeración	experience*		
			index*		
ListExperiences	Muestra una lista de una o más experiencias de Amazon Kendra. Puede crear una experiencia de Amazon Kendra como una aplicación de búsqueda	Enumeración	index*		
ListFaqs	Otorga permiso para enumerar las preguntas frecuentes	Enumeración	index*		
ListFeaturedResultsSets	Concede permiso para enumerar los conjuntos de resultados destacados	Enumeración	index*		
ListGroupsOlderThanOrderingId	Otorga permiso para enumerar los grupos que son más antiguos que un ID de pedido	Enumeración	index*		
			data-source		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIndices	Otorga permiso para enumerar los índices	Enumeración			
ListQuerySuggestionsBlockLists	Otorga permiso para incluir los QuerySuggestions BlockLists	Enumeración	index*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
ListThesauri	Otorga permiso para enumerar los diccionarios	Enumeración	index*		
PutPrincipalMapping	Otorga permiso para colocar el mapero de principales en el índice	Escritura	index*		
			data-source		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Query	Otorga permiso para consultar los documentos y las preguntas frecuentes	Lectura	index*		
Retrieve	Concede permiso para recuperar contenido relevante de un índice	Lectura	index*		
StartDataSourceSyncJob	Otorga permiso para iniciar el trabajo de sincronización de orígenes de datos	Escritura	data-source*		
			index*		
StopDataSourceSyncJob	Otorga permiso para detener el trabajo de sincronización de orígenes de datos	Escritura	data-source*		
			index*		
SubmitFeedback	Otorga permiso para enviar comentarios sobre los resultados de una consulta	Escritura	index*		
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	data-source		
			faq		
			featured-results-set		
			index		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			query-suggestions-block-list		
			thesaurus		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar de un recurso la etiqueta con la clave dada	Etiquetado	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccessControlConfiguration	Concede permiso para actualizar una configuración del control de acceso	Escritura	access-control-configuration*		
			index*		
UpdateDataSource	Concede permiso para actualizar un origen de datos	Escritura	data-source*		
			index*		
UpdateExperience	Actualiza su experiencia de Amazon Kendra, como una aplicación de búsqueda	Escritura	index*		
UpdateFeaturedResultsSet	Concede permiso para actualizar un conjunto de resultados destacados	Escritura	featured-results-set*		
			index*		
UpdateIndex	Otorga permiso para actualizar un índice	Escritura	index*		
UpdateQuerySuggestionsBlockList	Otorga permiso para actualizar un QuerySuggestions BlockList	Escritura	index*		
			query-suggestions-block-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQuerySuggestionsConfig	Otorga permiso para actualizar la configuración de sugerencias de consulta para un índice	Escritura	index*		
UpdateThesaurus	Otorga permiso para actualizar un diccionario	Escritura	index*		
			thesaurus*		

Tipos de recursos definidos por Amazon Kendra

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
index	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}`	aws:ResourceTag/${TagKey}
data-source	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/data-source/${DataSourceId}`	aws:ResourceTag/${TagKey}
faq	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/faq/${FaqId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
experience	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/experience/${ExperienceId}	
thesaurus	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/thesaurus/${ThesaurusId}	aws:ResourceTag/${TagKey}
query-suggestions-block-list	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/query-suggestions-block-list/${QuerySuggestionsBlockListId}	aws:ResourceTag/${TagKey}
featured-results-set	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/featured-results-set/${FeaturedResultsSetId}	aws:ResourceTag/${TagKey}
access-control-configuration	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/access-control-configuration/${AccessControlConfigurationId}	

Claves de condición para Amazon Kendra

Amazon Kendra define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking (prefijo de servicio: `kendra-ranking`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kendra Intelligent Ranking
- Tipos de recursos definidos por Amazon Kendra Intelligent Ranking
- Claves de condición para Amazon Kendra Intelligent Ranking

Acciones definidas por Amazon Kendra Intelligent Ranking

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRescoreExecutionPlan	Otorga permiso para crear un RescoreExecutionPlan	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRescoreExecutionPlan	Otorga permiso para eliminar un RescoreExecutionPlan	Escritura	rescore-execution-plan*		
DescribeRescoreExecutionPlan	Otorga permiso para describir un RescoreExecutionPlan	Lectura	rescore-execution-plan*		
ListRescoreExecutionPlans	Otorga permiso para enumerar todos RescoreExecutionPlans	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	rescore-execution-plan		
Rescore	Concede permiso para volver a puntuar documentos con Kendra Intelligent Ranking	Lectura	rescore-execution-plan*		
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	rescore-execution-plan		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar de un recurso la etiqueta con la clave dada	Etiquetado	rescore-execution-plan		
				aws:TagKeys	
UpdateRescoreExecutionPlan	Otorga permiso para actualizar un RescoreExecutionPlan	Escritura	rescore-execution-plan*		

Tipos de recursos definidos por Amazon Kendra Intelligent Ranking

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
rescore-execution-plan	`arn:${Partition}:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) (prefijo de servicio: `cassandra`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicas del servicio para utilizarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Keyspaces (for Apache Cassandra)
- Tipos de recursos definidos por Amazon Keyspaces (for Apache Cassandra)
- Claves de condición de Amazon Keyspaces (for Apache Cassandra)

Acciones definidas por Amazon Keyspaces (for Apache Cassandra)

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Alter	Otorga permiso para modificar un espacio de claves o una tabla.	Escritura	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
AlterMultiRegionResource	Concede permiso para modificar un espacio de claves o una tabla multirregión	Escritura	keyspace		
			table		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
Create	Otorga permiso para crear un espacio de claves o una tabla.	Escritura	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiRegionResource	Concede permiso para crear un espacio de claves o una tabla multirregión	Escritura	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Drop	Otorga permiso para soltar un espacio de claves o una tabla.	Escritura	keyspace		
			table		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DropMultiRegionResource	Concede permiso para eliminar un espacio de claves o una tabla multirregión	Escritura	keyspace		
			table		
GetRecords	Otorga permiso para recuperar los registros de transmisiones de los CDC de un fragmento determinado	Lectura	stream*		
GetShardIterator	Otorga permisos para devolver un iterador de fragmentos.	Lectura	stream*		
GetStream	Otorga permiso para devolver información sobre una transmisión de los CDC, incluida la composición de sus fragmentos	Lectura	stream*		
ListStreams	Otorga permiso para devolver una serie de transmisiones de los CDC ARNs asociadas a la cuenta corriente y al punto final	Enumeración			
Modify	Otorga permiso para INSERTAR, ACTUALIZAR o ELIMINAR datos de una tabla.	Escritura	table*		
ModifyMultiRegionResource	Concede permiso para INSERTAR, ACTUALIZAR o ELIMINAR datos de una tabla multirregión	Escritura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Restore	Otorga permiso para restaurar tabla a partir de una copia de seguridad	Escritura	table*		
RestoreMultiRegionTable	Concede permiso para restaurar una tabla multirregión a partir de una copia de seguridad	Escritura	table*		
Select	Otorga permiso para SELECCIONAR datos de una tabla.	Lectura	table*		
SelectMultiRegionResource	Concede permiso para SELECCIONAR datos de una tabla multirregión	Lectura	table*		
TagMultiRegionResource	Concede permiso para etiquetar un espacio de claves o una tabla multirregión	Etiquetado	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Otorga permiso para etiquetar un espacio clave, una tabla o una transmisión	Etiquetado	keyspace		
			stream		
			table		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagMultiRegionResource	Concede permiso para eliminar etiquetas de un espacio de claves o una tabla multirregión	Etiquetado	keyspace		
			table		
				aws:TagKeys	
UntagResource	Otorga permiso para quitar la etiqueta de un espacio clave, una tabla o una transmisión	Etiquetado	keyspace		
			stream		
			table		
				aws:TagKeys	
UpdatePartitioner	Otorga permiso para ACTUALIZAR el particionador en una tabla del sistema	Escritura	table*		

Tipos de recursos definidos por Amazon Keyspaces (for Apache Cassandra)

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
keyspace	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}/stream/${StreamLabel}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para Amazon Kinesis Analytics

Amazon Kinesis Analytics (prefijo de servicio: `kinesisanalytics`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kinesis Analytics
- Tipos de recursos definidos por Amazon Kinesis Analytics
- Claves de condición de Amazon Kinesis Analytics

Acciones definidas por Amazon Kinesis Analytics

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddApplicationInput	Concede permiso para agregar entradas a la aplicación	Escritura	application*		
AddApplicationOutput	Concede permiso para agregar resultados a la aplicación	Write	application*		
AddApplicationReferenceDataSource	Concede permiso para agregar un origen de datos de referencia a la aplicación	Escritura	application*		
CreateApplication	Concede permiso para crear una aplicación.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permiso para eliminar una aplicación	Escritura	application*		
DeleteApplicationOutput	Concede permiso para eliminar la salida especificada de la aplicación	Write	application*		
DeleteApplicationReferenceDataSource	Concede permiso para eliminar el origen de datos de referencia especificado de la aplicación	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeApplication	Concede permiso para describir la aplicación especificada	Lectura	application*		
DiscoverInputSchema	Concede permiso para descubrir el esquema de entrada para la aplicación	Lectura			
GetApplicationState [solo permiso]	Concede permiso a la consola de Kinesis Data Analytics para mostrar los resultados de la secuencia de las aplicaciones de tiempo de ejecución de Kinesis Data Analytics SQL	Lectura	application*		
ListApplications	Concede permiso para crear una lista de las aplicaciones para la cuenta	List			
ListTagsForResource	Concede permiso para obtener las etiquetas asociadas a la aplicación	Read	application*		
StartApplication	Concede permiso para iniciar la aplicación	Write	application*		
StopApplication	Concede permiso para detener la aplicación	Write	application*		
TagResource	Concede permiso para agregar etiquetas a la aplicación	Etiquetado	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas especificadas de la aplicación	Etiquetado	application*		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar la aplicación	Escritura	application*		

Tipos de recursos definidos por Amazon Kinesis Analytics

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Kinesis Analytics

Amazon Kinesis Analytics define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el par etiqueta-valor asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de claves de etiqueta obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 (prefijo de servicio: `kinesisanalytics`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kinesis Analytics V2
- Tipos de recurso definidos por Amazon Kinesis Analytics V2
- Claves de condición de Amazon Kinesis Analytics V2

Acciones definidas por Amazon Kinesis Analytics V2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddApplicationCloudWatchLoggingOption	Otorga permiso para agregar la opción de registro de CloudWatch a la aplicación	Write	application*		
AddApplicationInput	Otorga permiso para agregar entradas a la aplicación	Write	application*		
AddApplicationInputProcessingConfiguration	Otorga permiso para agregar configuración de procesamiento de entrada a la aplicación	Write	application*		
AddApplicationOutput	Concede permiso para agregar resultados a la aplicación	Write	application*		
AddApplicationReferenceDataSource	Concede permiso para agregar un origen de datos de referencia a la aplicación	Write	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddApplicationVpcConfiguration	Otorga permiso para agregar la configuración de VPC a la aplicación	Write	application*		
CreateApplication	Concede permiso para crear una aplicación.	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateApplicationPresignedUrl	Otorga permiso para crear y devolver una URL que puede usar para conectarse a la extensión de una aplicación	Read	application*		
CreateApplicationSnapshot	Otorga permiso para crear una instantánea para una aplicación	Write	application*		
DeleteApplication	Concede permiso para eliminar una aplicación	Write	application*		
DeleteApplicationCloudWatchLoggingOption	Otorga permiso para eliminar la opción de registro de CloudWatch especificada de la aplicación	Write	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApplicationInputProcessingConfiguration	Otorga permiso para eliminar la configuración de procesamiento de entrada especificada de la aplicación	Write	application*		
DeleteApplicationOutput	Concede permiso para eliminar la salida especificada de la aplicación	Write	application*		
DeleteApplicationReferenceDataSource	Concede permiso para eliminar el origen de datos de referencia especificado de la aplicación	Write	application*		
DeleteApplicationSnapshot	Otorga permiso para eliminar una instantánea de una aplicación	Write	application*		
DeleteApplicationVpcConfiguration	Otorga permiso para eliminar la configuración de VPC especificada de la aplicación	Write	application*		
DescribeApplication	Concede permiso para describir la aplicación especificada	Lectura	application*		
DescribeApplicationOperation	Concede permiso para describir una operación de una aplicación	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeApplicationSnapshot	Otorga permiso para describir una instantánea de la aplicación	Lectura	application*		
DescribeApplicationVersion	Otorga permiso para describir una versión de una aplicación	Lectura	application*		
DiscoverInputSchema	Concede permiso para descubrir el esquema de entrada para la aplicación	Lectura			iam:PassRole
ListApplicationOperations	Concede permiso para enumerar las operaciones de una aplicación	Lectura	application*		
ListApplicationSnapshots	Otorga permiso para crear una lista de las instantáneas de una aplicación	Lectura	application*		
ListApplicationVersions	Otorga permiso para enumerar una versión de aplicación	Lectura	application*		
ListApplications	Concede permiso para crear una lista de las aplicaciones para la cuenta	List			
ListTagsForResource	Concede permiso para obtener las etiquetas asociadas a la aplicación	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RollbackApplication	Otorga permiso para realizar una operación de restauración en una aplicación	Escritura	application*		
StartApplication	Concede permiso para iniciar la aplicación	Write	application*		
StopApplication	Concede permiso para detener la aplicación	Write	application*		
TagResource	Concede permiso para agregar etiquetas a la aplicación	Etiquetado	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas especificadas de la aplicación	Etiquetado	application*		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar la aplicación	Escritura	application*		
UpdateApplicationMaintenanceConfiguration	Otorga permiso para actualizar la configuración de mantenimiento de una aplicación	Escritura	application*		

Tipos de recurso definidos por Amazon Kinesis Analytics V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el par etiqueta-valor asociado con el recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por la presencia de claves de etiqueta obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Kinesis Data Streams

Amazon Kinesis Data Streams (prefijo de servicio: `kinesis`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kinesis Data Streams
- Tipos de recurso definidos por Amazon Kinesis Data Streams
- Claves de condición de Amazon Kinesis Data Streams

Acciones definidas por Amazon Kinesis Data Streams

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTagsToStream	Otorga permiso para agregar o actualizar etiquetas para el flujo de Amazon Kinesis especificado. Cada transmisión puede tener hasta 50 etiquetas	Etiquetado	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	Otorga permiso para crear un flujo de Amazon Kinesis	Escritura	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DecreaseStreamRetentionPeriod	Otorga permiso para reducir el periodo de retención de la transmisión, que es el periodo de tiempo en el que se puede acceder a los registros de datos después de agregarlos a la transmisión	Escritura	stream*	aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos asociada a una	Escritura	consumer*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	transmisión o un consumidor especificado		stream*	aws:ResourceTag/${TagKey}	
DeleteStream	Otorga permiso para eliminar un flujo y todos sus particiones y datos	Escritura	stream*	aws:ResourceTag/${TagKey}	
DeregisterStreamConsumer	Otorga permiso para anular el registro de un consumidor de flujos con un flujo de datos de Kinesis	Escritura	consumer*	aws:ResourceTag/${TagKey}	
DescribeLimits	Otorga permiso para describir los límites de los particiones y el uso de la cuenta	Lectura			
DescribeStream	Otorga permiso para describir el flujo especificado	Lectura	stream*	aws:ResourceTag/${TagKey}	
DescribeStreamConsumer	Otorga permiso para obtener la descripción de un consumidor de flujo registrado	Lectura	consumer*	aws:ResourceTag/${TagKey}	
DescribeStreamSummary	Otorga permiso para proporcionar una descripción resumida del flujo de datos de Kinesis especificado sin la lista de particiones	Lectura	stream*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableEnhancedMonitoring	Otorga permiso para desactivar la supervisión mejorada	Escritura			
EnableEnhancedMonitoring	Otorga permiso para habilitar la supervisión mejorada del flujo de datos de Kinesis para las métricas a nivel de particiones	Escritura			
GetRecords	Otorga permiso para obtener registros de datos de una partición	Lectura	stream*	aws:ResourceTag/${TagKey}	
GetResourcePolicy	Concede permiso para obtener una política de recursos asociada a una transmisión o un consumidor especificado	Lectura	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
GetShardIterator	Otorga permiso para obtener un iterador de particiones. Un iterador de particiones vence cinco minutos después de devolverse al solicitante	Lectura	stream*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
IncreaseStreamRetentionPeriod	Otorga permiso para aumentar el periodo de retención del flujo, que es el tiempo que los registros de datos son accesibles después de que sea agreguen al flujo	Escritura	stream*	aws:ResourceTag/${TagKey}	
ListShards	Otorga permiso para mostrar los fragmentos de un flujo y proporciona información sobre cada partición	Enumeración	stream*	aws:ResourceTag/${TagKey}	
ListStreamConsumers	Otorga permiso para mostrar los consumidores de flujos registrados para recibir datos de un flujo de Kinesis mediante el uso de una distribución mejorada, y proporciona información sobre cada consumidor	Enumeración	stream*	aws:ResourceTag/${TagKey}	
ListStreams	Otorga permiso para mostrar los flujos	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso de Amazon Kinesis especificado	Lectura	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForStream	Otorga permiso para mostrar las etiquetas del flujo de Amazon Kinesis especificado	Lectura	stream*	aws:ResourceTag/${TagKey}	
MergeShards	Otorga permiso para fusionar dos particiones adyacentes en un flujo y las combina en una sola partición para reducir la capacidad de ingesta y transporte de datos del flujo	Escritura	stream*	aws:ResourceTag/${TagKey}	
PutRecord	Otorga permiso para escribir un único registro de datos de un productor en una transmisión de Amazon Kinesis	Escritura	stream*	aws:ResourceTag/${TagKey}	
PutRecords	Otorga permiso para escribir varios registros de datos de un productor en una transmisión de Amazon Kinesis en una sola llamada (también denominada solicitud) PutRecords	Escritura	stream*	aws:ResourceTag/${TagKey}	
PutResourcePolicy	Concede permiso para asociar una política de recursos a una transmisión o un consumidor especificado	Escritura	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterStreamConsumer	Otorga permiso para registrar un consumidor de flujos con un flujo de datos de Kinesis	Escritura	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
RemoveTagsFromStream	Otorga permiso para eliminar etiquetas del flujo de datos de Kinesis especificado. Las etiquetas que se eliminan se borran y no se pueden recuperar después de que esta operación se complete correctamente	Etiquetado	stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
SplitShard	Otorga permiso para dividir una partición en dos nuevas particiones en el flujo de datos de Kinesis, a fin de aumentar la capacidad del flujo para ingerir y transportar datos	Escritura	stream*	aws:ResourceTag/${TagKey}	
StartStreamEncryption	Otorga permiso para habilitar o actualizar el cifrado del lado del servidor mediante una clave AWS KMS para una transmisión específica	Escritura	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopStreamEncryption	Otorga permiso para desactivar el cifrado del lado del servidor para un flujo determinado	Escritura	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	Otorga permiso para escuchar una partición específica con distribución mejorada	Lectura	consumer*	aws:ResourceTag/${TagKey}	
TagResource	Otorga permiso para añadir o actualizar etiquetas para el recurso de Amazon Kinesis especificado. Cada recurso puede tener hasta 50 etiquetas	Etiquetado	consumer*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar etiquetas del recurso de datos de Kinesis especificado. Las etiquetas que se eliminan se borran y no se pueden recuperar después de que esta operación se complete correctamente	Etiquetado	consumer*	aws:TagKeys aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateShardCount	Otorga permiso para actualizar el recuento de particiones del flujo especificado al número de particiones especificado	Escritura			
UpdateStreamMode	Otorga permiso para actualizar el modo de capacidad del flujo de datos	Escritura			

Tipos de recurso definidos por Amazon Kinesis Data Streams

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	aws:ResourceTag/${TagKey}
consumer	`arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}`	
kmsKey	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

Claves de condición de Amazon Kinesis Data Streams

Amazon Kinesis Data Streams define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Kinesis Firehose

Amazon Kinesis Firehose (prefijo de servicio: `firehose`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kinesis Firehose
- Tipos de recursos definidos por Amazon Kinesis Firehose
- Claves de condición para Amazon Kinesis Firehose

Acciones definidas por Amazon Kinesis Firehose

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeliveryStream	Otorga permiso para crear un flujo de entrega	Escritura	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDeliveryStream	Otorga permiso para eliminar un flujo de entrega y sus datos	Write	deliverystream*		
DescribeDeliveryStream	Otorga permiso para describir el flujo de entrega especificado y obtiene el estado	Lectura	deliverystream*		
ListDeliveryStreams	Otorga permiso para mostrar una lista de los flujos de entrega	Enumeración			
ListTagsForDeliveryStream	Otorga permiso para mostrar una lista de las etiquetas para el flujo de entrega especificado	Enumeración	deliverystream*		
PutRecord	Otorga permiso para escribir un único registro de datos en un flujo de entrega de Amazon Kinesis Firehose	Escritura	deliverystream*		
PutRecordBatch	Otorga permiso para escribir varios registros de datos en un flujo de entrega en una sola llamada, lo que puede lograr un rendimiento superior por productor que al escribir registros individuales	Escritura	deliverystream*		
StartDeliveryStreamEncryption	Otorga permiso para habilitar el cifrado del lado del servidor (SSE) para el flujo de entrega	Escritura	deliverystream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopDeliveryStreamEncryption	Otorga permiso para desactivar el destino especificado del flujo de entrega especificado	Escritura	deliverystream*		
TagDeliveryStream	Otorga permiso para agregar o actualizar etiquetas para el flujo de entrega especificado	Etiquetado	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	Otorga permiso para quitar etiquetas del flujo de entrega especificado	Etiquetado	deliverystream*		
				aws:TagKeys	
UpdateDestination	Otorga permiso para actualizar el destino especificado del flujo de entrega especificado	Escritura	deliverystream*		

Tipos de recursos definidos por Amazon Kinesis Firehose

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Kinesis Firehose

Amazon Kinesis Firehose define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Kinesis Video Streams

Amazon Kinesis Video Streams (prefijo de servicio: `kinesisvideo`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Kinesis Video Streams
- Tipos de recurso definidos por Amazon Kinesis Video Streams
- Claves de condición de Amazon Kinesis Video Streams

Acciones definidas por Amazon Kinesis Video Streams

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConnectAsMaster	Otorga permiso para conectarse como maestro al canal de señalización especificado por el punto de enlace.	Write	channel*		
ConnectAsViewer	Otorga permiso para conectarse como lector al canal de señalización especificado por el punto de enlace.	Write	channel*		
CreateSignalingChannel	Otorga permiso para crear un canal de señalización.	Write	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Otorga permiso para crear una transmisión de vídeo de Kinesis.	Escritura	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEdgeConfiguration	Concede permiso para eliminar la configuración de periferia de su secuencia de video de Kinesis	Escritura	stream*		
DeleteSignalingChannel	Otorga permiso para eliminar un canal de señalización existente.	Write	channel*		
DeleteStream	Otorga permiso para eliminar una transmisión de vídeo de Kinesis existente.	Escritura	stream*		
DescribeEdgeConfiguration	Otorga permiso para describir la configuración de periferia de su flujo de video de Kinesis	Lectura	stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeImageGenerationConfiguration	Otorga permiso para describir la configuración de generación de imágenes de su transmisión de video de Kinesis	Lectura	stream*		
DescribeMappedResourceConfiguration	Otorga permiso para describir el recurso asignado a la transmisión de video de Kinesis	Enumeración	stream*		
DescribeMediaStorageConfiguration	Otorga permiso para describir la configuración de almacenamiento de un canal de señalización	Lectura	channel*		
DescribeNotificationConfiguration	Otorga permiso para describir la configuración de notificación de su transmisión de video de Kinesis	Lectura	stream*		
DescribeSignalingChannel	Otorga permiso para describir el canal de señalización especificado	List	channel*		
DescribeStream	Otorga permiso para describir la transmisión de vídeo de Kinesis especificada	List	stream*		
GetClip	Otorga permiso para obtener un clip multimedia de una transmisión de video	Read	stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDASHStreamingSessionURL	Otorga permiso para crear una URL para transmitir vídeo MPEG-DASH	Read	stream*		
GetDataEndpoint	Otorga permiso para obtener un punto de enlace para una transmisión específica para leer o escribir datos multimedia en Kinesis Video Streams	Read	stream*		
GetHLSStreamingSessionURL	Otorga permiso para crear una URL para transmitir vídeo HLS	Read	stream*		
GetIceServerConfig	Otorga permiso para obtener la configuración del servidor ICE	Lectura	channel*		
GetImages	Otorga permiso para obtener imágenes generadas por la transmisión de video de Kinesis	Lectura	stream*		
GetMedia	Otorga permiso para devolver contenido multimedia de una transmisión de vídeo de Kinesis	Read	stream*		
GetMediaForFragmentList	Otorga permiso para leer y devolver datos multimedia solo desde el almacenamiento persistente	Read	stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSignalingChannelEndpoint	Otorga permiso para obtener puntos de enlace para una combinación específica de protocolo y rol para un canal de señalización	Lectura	channel*		
JoinStorageSession	Otorga permiso para unirse a una sesión de almacenamiento de un canal	Escritura	channel*		
JoinStorageSessionAsViewer	Concede permiso para unirse a una sesión de almacenamiento para un canal como espectador	Escritura	channel*		
ListEdgeAgentConfigurations	Concede permiso para obtener las configuraciones de un agente de periferia	Enumeración			
ListFragments	Otorga permiso para enumerar los fragmentos del almacenamiento de archivo en función del token de paginación o del tipo de selector con el rango especificado	List	stream*		
ListSignalingChannels	Otorga permiso para enumerar los canales de señalización	List			
ListStreams	Otorga permiso para enumerar las transmisiones de vídeo de Kinesis	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para obtener las etiquetas asociadas con el recurso	Read	channel		
			stream		
ListTagsForStream	Otorga permiso para obtener las etiquetas asociadas a la transmisión de vídeo de Kinesis	Read	stream*		
PutMedia	Otorga permiso para enviar datos multimedia a una transmisión de vídeo de Kinesis	Write	stream*		
SendAlexaOfferToMaster	Otorga permiso para enviar la oferta Alexa SDP al maestro	Escritura	channel*		
StartEdgeConfigurationUpdate	Otorga permiso para iniciar la actualización de la configuración de periferia de su flujo de video de Kinesis	Escritura	stream*		
TagResource	Otorga permiso para asociar un conjunto de etiquetas al recurso	Etiquetado	channel		
			stream		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagStream	Otorga permiso para asociar un conjunto de etiquetas a sus transmisiones de video de Kinesis	Etiquetado	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una o varias etiquetas de un recurso	Etiquetado	channel		
			stream		
				aws:TagKeys	
UntagStream	Otorga permiso para eliminar una o más etiquetas de sus transmisiones de video de Kinesis	Etiquetado	stream*		
				aws:TagKeys	
UpdateDataRetention	Otorga permiso para actualizar el periodo de retención de datos de su transmisión de vídeo de Kinesis	Escritura	stream*		
UpdateImageGenerationConfiguration	Otorga permiso para actualizar la configuración de generación de imágenes de su transmisión de video de Kinesis	Escritura	stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMediaStorageConfiguration	Otorga permiso para crear o actualizar una asignación entre una transmisión y un canal de señalización	Escritura	channel*		
UpdateNotificationConfiguration	Otorga permiso para actualizar la configuración de notificación de su transmisión de video de Kinesis	Escritura	stream*		
UpdateSignalingChannel	Otorga permiso para actualizar un canal de señalización existente	Write	channel*		
UpdateStream	Otorga permiso para actualizar una transmisión de vídeo de Kinesis existente	Write	stream*		

Tipos de recurso definidos por Amazon Kinesis Video Streams

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
stream	`arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Kinesis Video Streams

Amazon Kinesis Video Streams define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra solicitudes en función del conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra las acciones en función del valor-etiqueta asociado con la transmisión	Cadena
aws:TagKeys	Filtra las solicitudes en función de la presencia de claves de etiqueta obligatorias en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS Lake Formation

AWS Lake Formation (prefijo de servicio:`lakeformation`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Lake Formation
- Tipos de recursos definidos por AWS Lake Formation
- Claves de condición para AWS Lake Formation

Acciones definidas por AWS Lake Formation

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddLFTagsToResource	Otorga permiso para adjuntar etiquetas Lake Formation a recursos de catálogo	Etiquetado			
BatchGrantPermissions	Otorga el permiso para los permisos de lago de datos a una o varias entidades principales en un lote	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchRevokePermissions	Otorga el permiso para revocar los permisos del lago de datos de una o varias entidades principales en un lote	Administración de permisos			
CancelTransaction	Otorga permiso para cancelar la transacción dada	Escritura			
CommitTransaction	Otorga permiso para confirmar la transacción dada	Escritura			
CreateDataCellsFilter	Otorga permiso para crear un filtro de celdas de datos de Lake Formation	Escritura			
CreateLFTag	Otorga permiso para crear una etiqueta Lake Formation	Escritura			
CreateLFTagExpression	Otorga permiso para crear una expresión de etiqueta de Lake Formation	Escritura			
CreateLakeFormationIdentityCenterConfiguration	Concede permiso para crear una conexión de IAM Identity Center con Lake Formation para permitir que los usuarios y grupos de IAM Identity Center accedan a los recursos de Data Catalog	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLakeFormationOptIn	Exige los permisos de Lake Formation para las bases de datos, tablas y entidades principales dados	Escritura			
DeleteDataCellsFilter	Otorga permiso para eliminar un filtro de celdas de datos de Lake Formation	Escritura			
DeleteLFTag	Otorga permiso para eliminar una etiqueta Lake Formation	Escritura			
DeleteLFTagExpression	Otorga permiso para eliminar una expresión de Lake Formation	Escritura			
DeleteLakeFormationIdentityCenterConfiguration	Concede permiso para eliminar una conexión de IAM Identity Center con Lake Formation	Escritura			
DeleteLakeFormationOptIn	Concede permiso para eliminar la aplicación de permisos de Lake Formation de las bases de datos, tablas y entidades de seguridad dadas	Escritura			
DeleteObjectsOnCancel	Otorga permiso para eliminar los objetos especificados si la transacción se cancela	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterResource	Otorga el permiso para dar de baja una ubicación registrada	Escritura			
DescribeLakeFormationIdentityCenterConfiguration	Concede permiso para describir la conexión de IAM Identity Center con Lake Formation	Lectura			
DescribeResource	Otorga el permiso para describir una ubicación registrada	Lectura			
DescribeTransaction	Otorga permiso para obtener el estado de la transacción dada	Lectura			
ExtendTransaction	Otorga permiso para ampliar el tiempo de espera de la transacción dada	Escritura			
GetDataAccess	Otorga el permiso de acceso al lago de datos virtual	Escritura		lakeformation:EnabledOnlyForMetaDataAccess	
GetDataCellsFilter	Concede permiso para recuperar un filtro de celdas de datos de Lake Formation	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDataLakePrincipal	Concede permiso para recuperar la identidad de la entidad principal que invoca	Lectura			
GetDataLakeSettings	Otorga el permiso para recuperar la configuración del lago de datos, como la lista de administradores del lago de datos y los permisos predeterminados de la base de datos y la tabla	Lectura			
GetEffectivePermissionsForPath	Otorga permiso para recuperar los permisos adjuntados a los recursos de la ruta especificada	Lectura			
GetLFTag	Otorga permiso para recuperar una etiqueta Lake Formation	Lectura			
GetLFTagExpression	Otorga permiso para recuperar una expresión de etiqueta de Lake Formation	Lectura			
GetQueryState	Otorga permiso para recuperar el estado de la consulta dada	Lectura			lakeformation:StartQueryPlanning

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueryStatistics	Otorga permiso para recuperar las estadísticas de la consulta dada	Lectura			lakeformation:StartQueryPlanning
GetResourceLFTags	Otorga el permiso para recuperar etiquetas Lakeformation en un recurso de catálogo	Lectura			
GetTableObjects	Otorga permiso para recuperar objetos de una tabla	Lectura			
GetWorkUnitResults	Otorga permiso para recuperar los resultados de las unidades de trabajo dadas	Lectura			lakeformation:GetWorkUnits lakeformation:StartQueryPlanning
GetWorkUnits	Otorga permiso para recuperar las unidades de trabajo de la consulta dada	Lectura			lakeformation:StartQueryPlanning
GrantPermissions	Otorga el permiso para los permisos de lago de datos a una entidad principal	Administración de permisos			
ListDataCellsFilter	Otorga permiso para enumerar filtros de celda	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLFTagExpressions	Otorga permiso para enumerar las expresiones de las etiquetas de Lake Formation	Lectura			
ListLFTags	Otorga permiso para enumerar etiquetas Lake Formation	Lectura			
ListLakeFormationOptIns	Concede permiso para recuperar la lista actual de recursos y entidades principales que han sido habilitadas para aplicar los permisos de Lake Formation	Enumeración			
ListPermissions	Otorga el permiso para crear una lista de permisos filtrados por una entidad principal o un recurso	Enumeración			
ListResources	Otorga el permiso para crear una lista de ubicaciones registradas	Enumeración			
ListTableStorageOptimizers	Otorga permiso para enumerar todos los optimizadores de almacenamiento de información para la tabla regida	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTransactions	Otorga permiso para enumerar todas las transacciones del sistema	Enumeración			
PutDataLakeSettings	Otorga el permiso para sobrescribir la configuración del lago de datos, como la lista de administradores del lago de datos y los permisos predeterminados de la base de datos y la tabla	Administración de permisos			
RegisterResource	Otorga el permiso para registrar una ubicación nueva que Lake Formation va a administrar	Escritura			
RegisterResourceWithPrivilegedAccess	Otorga permiso para registrar una nueva ubicación que será administrada por Lake Formation, con acceso privilegiado	Escritura			
RemoveLFTagsFromResource	Otorga el permiso para eliminar etiquetas Lakeformation de recursos de catálogo	Etiquetado			
RevokePermissions	Otorga el permiso para revocar los permisos de lago de datos de una entidad principal	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchDatabasesByLFTags	Otorga permiso para enumerar las bases de datos de catálogo con etiquetas Lake Formation	Lectura			
SearchTablesByLFTags	Otorga permiso para enumerar las tablas de catálogo con etiquetas Lake Formation	Lectura			
StartQueryPlanning	Otorga permiso para iniciar la planificación de la consulta dada	Escritura			
StartTransaction	Otorga permiso para iniciar una nueva transacción	Escritura			
UpdateDataCellsFilter	Concede permiso para actualizar un filtro de celdas de datos de Lake Formation	Escritura			
UpdateLFTag	Otorga permiso para actualizar una etiqueta Lake Formation	Escritura			
UpdateLFTagExpression	Otorga permiso para actualizar una expresión de Lake Formation	Escritura			
UpdateLakeFormationIdentityCenterConfiguration	Concede permiso para actualizar los parámetros de conexión de IAM Identity Center	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateResource	Otorga el permiso para actualizar una ubicación registrada	Escritura			
UpdateTableObjects	Otorga permiso para agregar o eliminar los objetos especificados en o desde una tabla	Escritura			
UpdateTableStorageOptimizer	Otorga permiso para actualizar la configuración del optimizador de almacenamiento para la tabla regida	Escritura			

Tipos de recursos definidos por AWS Lake Formation

AWS Lake Formation no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Lake Formation, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Lake Formation

AWS Lake Formation define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
lakeformation:EnabledOnlyForMetaDataAccess	Filtra el acceso según la presencia de la clave configurada para la política basada en la identidad del rol	Bool

Acciones, recursos y claves de condición para AWS Lambda

AWS Lambda (prefijo de servicio:`lambda`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Lambda
- Tipos de recursos definidos por AWS Lambda
- Claves de condición para AWS Lambda

Acciones definidas por AWS Lambda

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddLayerVersionPermission	Otorga permiso para añadir permisos a la política basada en recursos de una versión de una capa Lambda AWS	Administración de permisos	layerVersion*		
AddPermission	Otorga permiso para dar permiso a un AWS servicio o a otra cuenta para usar una función AWS Lambda	Administración de permisos	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
CreateAlias	Concede permiso para crear un alias para una versión de función de Lambda	Escritura	function*		
CreateCodeSigningConfig	Otorga permiso para crear una configuración de firma de código AWS Lambda	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	Otorga permiso para crear un mapeo entre una fuente de eventos y una AWS función Lambda	Escritura		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFunction	Concede permiso para crear una función AWS Lambda	Escritura	function*		iam:PassRole
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionUrlConfig	Concede permiso para crear una configuración de url de función para una función Lambda	Escritura	function*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteAlias	Concede permiso para eliminar un alias de AWS función Lambda	Escritura	function*		
DeleteCodeSigningConfig	Otorga permiso para eliminar una configuración de firma de código AWS Lambda	Escritura	codesigningconfig*		
DeleteEventSourceMapping	Otorga permiso para eliminar un mapeo de origen de eventos de AWS Lambda	Escritura	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Concede permiso para eliminar una función AWS Lambda	Escritura	function*		
DeleteFunctionCodeSigningConfig	Otorga permiso para separar una configuración de firma de código de una función AWS Lambda	Escritura	function*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFunctionConcurrency	Concede permiso para eliminar un límite de ejecución simultánea de una función AWS Lambda	Escritura	function*		
DeleteFunctionEventInvokeConfig	Concede permiso para eliminar la configuración de la invocación asíncrona de una función, versión o alias de AWS Lambda	Escritura	function*		
DeleteFunctionUrlConfig	Concede permiso para eliminar configuración de url de función para una función Lambda	Escritura	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	Concede permiso para eliminar una versión de una capa AWS Lambda	Escritura	layerVersion*		
DeleteProvisionedConcurrencyConfig	Concede permiso para eliminar la configuración de simultaneidad aprovisionada para una función Lambda AWS	Escritura	function alias		
			function version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableReplication [solo permiso]	Concede permiso para desactivar la replicación para una función de Lambda@Edge	Permissions management	function*		
EnableReplication [solo permiso]	Concede permiso para habilitar la replicación para una función de Lambda@Edge	Administración de permisos	function*		
GetAccountSettings	Otorga permiso para ver los detalles sobre los límites y el uso de una cuenta en un Región de AWS	Lectura			
GetAlias	Otorga permiso para ver detalles sobre un alias de AWS función Lambda	Lectura	function*		
GetCodeSigningConfig	Otorga permiso para ver los detalles de una configuración de firma de código AWS Lambda	Lectura	code signing config*		
GetEventSourceMapping	Otorga permiso para ver detalles sobre un mapeo de origen de eventos de AWS Lambda	Lectura	eventSourceMapping*		
				lambda:FunctionArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFunction	Otorga permiso para ver detalles sobre una AWS función Lambda	Lectura	function*		
GetFunctionCodeSigningConfig	Otorga permiso para ver el arn de configuración de firma de código adjunto a una función AWS Lambda	Lectura	function*		
GetFunctionConcurrency	Concede permiso para ver detalles sobre la configuración de simultaneidad reservada para una función	Lectura	function*		
GetFunctionConfiguration	Otorga permiso para ver detalles sobre los ajustes específicos de la versión de una función o versión de AWS Lambda	Lectura	function*		
GetFunctionEventInvokeConfig	Concede permiso para ver la configuración de invocación asincrónica de una función, versión o alias	Lectura	function*		
GetFunctionRecursionConfig	Otorga permiso para ver la configuración de recursión de una función AWS Lambda	Lectura	function*		
GetFunctionUrlConfig	Concede permiso para leer la configuración url de función para una función Lambda	Lectura	function*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				lambda:FunctionUrlAuthType lambda:FunctionArn	
GetLayerVersion	Otorga permiso para ver detalles sobre una versión de una AWS capa Lambda. Tenga en cuenta que esta acción también es compatible con GetLayerVersionByArn la API	Lectura	layerVersion*		
GetLayerVersionPolicy	Otorga permiso para ver la política basada en recursos de una versión de una capa Lambda AWS	Lectura	layerVersion*		
GetPolicy	Otorga permiso para ver la política basada en recursos de una función, versión o alias de AWS Lambda	Lectura	function*		
GetProvisionedConcurrencyConfig	Otorga permiso para ver la configuración de simultaneidad aprovisionada para el alias o la versión de una función de AWS Lambda	Lectura	functionalias		
			functionversion		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRuntimeManagementConfig	Otorga permiso para ver la configuración de administración del tiempo de ejecución de una AWS función Lambda	Lectura	function*		
InvokeAsync	Concede permiso para invocar una función de forma asíncrona (Obsoleto)	Escritura	function*		
InvokeFunction	Otorga permiso para invocar una función AWS Lambda	Escritura	function*		
				lambda:EventSourceToken	
InvokeFunctionUrl [solo permiso]	Otorga permiso para invocar una función AWS Lambda a través de una URL	Escritura	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	Concede permiso para recuperar una lista de alias para una función AWS Lambda	Enumeración	function*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCodeSigningConfigs	Concede permiso para recuperar una lista de configuraciones de AWS firma de código Lambda	Enumeración			
ListEventSourceMappings	Otorga permiso para recuperar una lista de mapeos de AWS fuentes de eventos Lambda	Enumeración			
ListFunctionEventInvokeConfigs	Concede permiso para recuperar una lista de configuraciones para la invocación asíncrona de una función	Enumeración	function*		
ListFunctionUrlConfigs	Concede permiso para leer las configuraciones de url de funciones para una función	Enumeración	function*		
				lambda:FunctionUrlAuthType	
ListFunctions	Concede permiso para recuperar una lista de funciones AWS Lambda, con la configuración específica de cada versión de cada función	Enumeración			
ListFunctionsByCodeSigningConfig	Otorga permiso para recuperar una lista de funciones AWS Lambda mediante la configuración de firma de código asignada	Enumeración	code signing config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLayerVersions	Otorga permiso para recuperar una lista de versiones de una capa AWS Lambda	Enumeración			
ListLayers	Otorga permiso para recuperar una lista de capas AWS Lambda, con detalles sobre la última versión de cada capa	Enumeración			
ListProvisionedConcurrencyConfigs	Otorga permiso para recuperar una lista de configuraciones de simultaneidad aprovisionadas para una función Lambda AWS	Enumeración	function*		
ListTags	Otorga permiso para recuperar una lista de etiquetas para un recurso de configuración de función AWS Lambda, mapeo de fuentes de eventos o firma de código	Lectura	codesigningconfig		
			eventSourceMapping		
			function		
ListVersionsByFunction	Concede permiso para recuperar una lista de versiones de una función AWS Lambda	Enumeración	function*		
PublishLayerVersion	Otorga permiso para crear una AWS capa Lambda	Escritura	layer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PublishVersion	Concede permiso para crear una versión de la AWS función Lambda	Escritura	function*		
PutFunctionCodeSigningConfig	Otorga permiso para adjuntar una configuración de firma de código a una AWS función Lambda	Escritura	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Concede permiso para configurar la simultaneidad reservada para una función AWS Lambda	Escritura	function*		
PutFunctionEventInvokeConfig	Otorga permiso para configurar opciones para la invocación asíncrona en una función, versión o alias de AWS Lambda	Escritura	function*		
PutFunctionRecursionConfig	Concede permiso para actualizar la configuración de recursión de una función AWS Lambda	Escritura	function*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutProvisionedConcurrencyConfig	Otorga permiso para configurar la simultaneidad aprovisionada para el alias o la versión de una función de AWS Lambda	Escritura	function alias		
			function version		
PutRuntimeManagementConfig	Concede permiso para actualizar la configuración de administración del tiempo de ejecución de una AWS función Lambda	Escritura	function*		
RemoveLayerVersionPermission	Concede permiso para eliminar una declaración de la política de permisos de una versión de una capa AWS Lambda	Administración de permisos	layerVersion*		
RemovePermission	Otorga permiso para revocar el permiso de uso de funciones de un AWS servicio u otra cuenta	Administración de permisos	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
TagResource	Otorga permiso para añadir etiquetas a un recurso de configuración de función AWS Lambda, mapeo de fuentes de eventos o firma de código	Etiquetado	code signing config		
			eventSourceMapping		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			function		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de configuración de funciones AWS Lambda, fuentes de eventos, mapeo o firma de código	Etiquetado	code signing config		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	Concede permiso para actualizar la configuración del alias de una función AWS Lambda	Escritura	function*		
UpdateCodeSigningConfig	Otorga permiso para actualizar una configuración de firma de código AWS Lambda	Escritura	code signing config*		
UpdateEventSourceMapping	Otorga permiso para actualizar la configuración de un mapeo de origen de eventos AWS Lambda	Escritura	eventSourceMapping*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				lambda:FunctionArn	
UpdateFunctionCode	Concede permiso para actualizar el código de una función AWS Lambda	Escritura	function*		
UpdateFunctionCodeSigningConfig	Concede permiso para actualizar la configuración de firma de código de una función AWS Lambda	Escritura	codesigningconfig*		
			function*		
UpdateFunctionConfiguration	Otorga permiso para modificar la configuración específica de la versión de una función Lambda AWS	Escritura	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	Otorga permiso para modificar la configuración de la invocación asíncrona de una función, versión o alias de AWS Lambda	Escritura	function*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFunctionUrlConfig	Concede permiso para actualizar una configuración de url de función para una función Lambda	Escritura	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Tipos de recursos definidos por AWS Lambda

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
code signing config	`arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}`	aws:ResourceTag/${TagKey}
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	aws:ResourceTag/${TagKey}
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
function alias	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}`	aws:ResourceTag/${TagKey}
function version	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}`	aws:ResourceTag/${TagKey}
layer	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}`	
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	

Claves de condición para AWS Lambda

AWS Lambda define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
lambda:CodeSigningConfigArn	Filtra el acceso por el ARN de una configuración de firma de código AWS Lambda	ARN
lambda:EventSourceToken	Filtra el acceso por el ID desde una fuente sin AWS eventos configurada para la función AWS Lambda	Cadena
lambda:FunctionArn	Filtra el acceso por el ARN de una función Lambda AWS	ARN
lambda:FunctionUrlAuthType	Filtra el acceso por tipo de autorización especificado en la solicitud Disponible durante CreateFunctionUrlConfig las UpdateFunctionUrlConfig operaciones, DeleteFunctionUrlConfig, GetFunctionUrlConfig ListFunctionUrlConfig, y AddPermission RemovePermission	Cadena
lambda:Layer	Filtra el acceso por el ARN de una versión de una capa Lambda AWS	ArrayOfString
lambda:Principal	Filtra el acceso restringiendo el AWS servicio o la cuenta que puede invocar una función	Cadena
lambda:SecurityGroupIds	Filtra el acceso por el identificador de los grupos de seguridad configurados para la AWS función Lambda	ArrayOfString
lambda:SourceFunctionArn	Filtra el acceso por el ARN de la función AWS Lambda desde la que se originó la solicitud	ARN
lambda:SubnetIds	Filtra el acceso por el identificador de las subredes configuradas para la función AWS Lambda	ArrayOfString
lambda:VpcIds	Filtra el acceso por el ID de la VPC configurada para la función Lambda AWS	Cadena

Acciones, recursos y claves de condición para AWS Launch Wizard

AWS Launch Wizard (prefijo de servicio:`launchwizard`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Launch Wizard
- Tipos de recursos definidos por AWS Launch Wizard
- Claves de condición para AWS Launch Wizard

Acciones definidas por AWS Launch Wizard

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAdditionalNode [solo permiso]	Concede permiso para crear un nodo adicional	Escritura			
CreateDeployment	Concede permiso para crear una implementación.	Escritura	deployment*	aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateSettingsSet [solo permiso]	Concede permiso para crear un conjunto de configuración de una aplicación	Escritura			
DeleteAdditionalNode [solo permiso]	Concede permiso para eliminar un nodo adicional	Escritura			
DeleteApp [solo permiso]	Concede permiso para eliminar una aplicación.	Escritura			
DeleteDeployment	Concede permiso para eliminar una implementación	Escritura	deployment*	aws:ResourceTag/${TagKey}	
DeleteSettingsSet [solo permiso]	Concede permiso para eliminar un conjunto de ajustes	Escritura			
DescribeAdditionalNode [solo permiso]	Concede permiso para describir un nodo adicional	Lectura			
DescribeProvisionedApp [solo permiso]	Concede permiso para describir aplicaciones de aprovisionamiento	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeProvisioningEvents [solo permiso]	Concede permiso para describir eventos de aprovisionamiento	Lectura			
DescribeSettingsSet [solo permiso]	Concede permiso para describir un conjunto de configuración de una aplicación	Lectura			
GetDeployment	Concede permiso para obtener una implementación.	Lectura	deployment*	aws:ResourceTag/${TagKey}	
GetInfrastructureSuggestion [solo permiso]	Concede permiso para obtener una sugerencia de infraestructura	Lectura			
GetIpAddress [solo permiso]	Concede permiso para obtener la dirección IP del cliente	Lectura			
GetResourceCostEstimate [solo permiso]	Concede permiso para obtener una estimación de costo de recurso	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourceRecommendation [solo permiso]	Concede permiso para obtener una recomendación para un recurso	Lectura			
GetSettingsSet [solo permiso]	Concede permiso para obtener un conjunto de ajustes	Lectura			
GetWorkload	Concede permiso para obtener una carga de trabajo	Lectura			
GetWorkloadAsset [solo permiso]	Concede permiso para obtener activos de carga de trabajo	Lectura			
GetWorkloadAssets [solo permiso]	Concede permiso para obtener activos de carga de trabajo	Lectura			
GetWorkloadDeploymentPattern	Concede permiso para obtener un patrón de implementación	Lectura			
ListAdditionalNodes [solo permiso]	Concede permiso para enumerar nodos adicionales	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAllowedResources [solo permiso]	Concede permiso para enumerar los recursos permitidos	Enumeración			
ListDeploymentEvents	Concede permiso para enumerar los eventos que se produjeron durante una implementación	Enumeración			
ListDeployments	Otorga permiso para enumerar implementaciones	Enumeración			
ListProvisionedApps [solo permiso]	Concede permiso para enumerar aplicaciones de aprovisionamiento	Enumeración			
ListResourceCostEstimates [solo permiso]	Concede permiso para enumerar estimaciones de costos de recursos	Enumeración			
ListSettingsSets [solo permiso]	Concede permiso para enumerar el conjunto de ajustes	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un LaunchWizard recurso.	Lectura	deployment	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorkloadDeploymentOptions [solo permiso]	Concede permiso para enumerar las opciones de implementación de una carga de trabajo determinada	Enumeración			
ListWorkloadDeploymentPatterns	Concede permiso para enumerar los patrones de implementación de una carga de trabajo	Enumeración			
ListWorkloads	Concede permiso para enumerar cargas de trabajo	Enumeración			
PutSettingsSet [solo permiso]	Concede permiso para crear un conjunto de ajustes	Escritura			
StartProvisioning [solo permiso]	Concede permiso para iniciar un aprovisionamiento	Escritura			
TagResource	Otorga permiso para etiquetar un LaunchWizard recurso.	Etiquetado	deployment	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para quitar la etiqueta de un LaunchWizard recurso.	Etiquetado	deployment	aws:TagKeys	
UpdateSettingsSet [solo permiso]	Concede permiso para actualizar un conjunto de configuración de una aplicación	Escritura			

Tipos de recursos definidos por AWS Launch Wizard

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
deployment	`arn:${Partition}:launchwizard:${Region}:${Account}:deployment/${DeploymentId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Launch Wizard

AWS Launch Wizard define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso en función de pares de clave-valor asociados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Lex

Amazon Lex (prefijo de servicio: `lex`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Lex
- Tipos de recurso definidos por Amazon Lex
- Claves de condición de Amazon Lex

Acciones definidas por Amazon Lex

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBotVersion	Crea una nueva versión basada en la versión $LATEST del bot especificado	Escritura	bot version*		
CreateIntentVersion	Crea una nueva versión basada en la versión $LATEST de la intención especificada	Escritura	intent version*		
CreateSlotTypeVersion	Crea una nueva versión basada en la versión $LATEST del tipo de ranura especificado	Escritura	slottype version*		
DeleteBot	Elimina todas las versiones un bot	Escritura	bot version*		
DeleteBotAlias	Elimina un alias para un bot específico	Escritura	bot alias*		
DeleteBotChannelAssociation	Elimina la asociación entre un alias de bot de Amazon Lex y una plataforma de mensajería	Escritura	channel*		
DeleteBotVersion	Elimina una versión específica de un bot	Escritura	bot version*		
DeleteIntent	Elimina todas las versiones una intención	Escritura	intent version*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIntentVersion	Elimina una versión específica de una intención	Escritura	intent version*		
DeleteSession	Elimina la información de sesión de un bot, alias e ID de usuario especificados	Escritura	bot alias		
			bot version		
DeleteSlotType	Elimina todas las versiones de un tipo de ranura	Escritura	slottype version*		
DeleteSlotTypeVersion	Elimina una versión específica de un tipo de ranura	Escritura	slottype version*		
DeleteUtterances	Elimina la información que Amazon Lex mantiene para enunciados en un bot específico y userId	Escritura	bot version*		
GetBot	Devuelve la información de un bot específico. Además del nombre del bot, se requiere la versión del bot o el alias	Lectura	bot alias		
			bot version		
GetBotAlias	Devuelve información sobre un alias de bot de Amazon Lex	Lectura	bot alias*		
GetBotAliases	Devuelve una lista de alias para un bot de Amazon Lex determinado	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBotChannelAssociation	Devuelve información sobre la asociación entre un bot de Amazon Lex y una plataforma de mensajería	Lectura	channel*		
GetBotChannelAssociations	Devuelve una lista de todos los canales asociados con un único bot	Enumeración	channel*		
GetBotVersions	Devuelve información sobre todas las versiones de un bot específico	Enumeración	bot version*		
GetBots	Devuelve información de la versión $LATEST de todos los bots, sujeta a filtros proporcionados por el cliente	Enumeración			
GetBuiltinIntent	Devuelve información sobre una intención integrada	Lectura			
GetBuiltinIntents	Obtiene una lista de las intenciones integradas que cumplen los criterios especificados	Lectura			
GetBuiltinSlotTypes	Obtiene una lista de tipos de ranura integradas que cumplen los criterios especificados	Lectura			
GetExport	Exporta recursos de Amazon Lex en un formato solicitado	Lectura	bot version*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetImport	Obtiene información sobre un trabajo de importación iniciado con StartImport	Lectura			
GetIntent	Devuelve la información de una intención específica. Además del nombre de la intención, también debe especificar la versión de la intención	Lectura	intent version*		
GetIntentVersions	Devuelve información sobre todas las versiones de una intención específica	Enumeración	intent version*		
GetIntents	Devuelve información de la versión $LATEST de todas las intenciones, sujeta a filtros proporcionados por el cliente	Enumeración			
GetMigration	Otorga permiso para ver una migración en curso o completada	Lectura			
GetMigrations	Otorga permiso para ver la lista de migraciones de Amazon Lex v1 a Amazon Lex v2	Enumeración			
GetSession	Devuelve la información de sesión de un bot, alias e ID de usuario especificados	Lectura	bot alias		
			bot version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSlotType	Devuelve información sobre una versión específica de un tipo de ranura. Además de especificar el nombre del tipo de ranura, también debe especificar la versión del tipo de ranura	Lectura	slottype version*		
GetSlotTypeVersions	Devuelve información sobre todas las versiones de un tipo de ranura específico	Enumeración	slottype version*		
GetSlotTypes	Devuelve información de la versión $LATEST de todos los tipos de ranuras, sujeta a filtros proporcionados por el cliente	Enumeración			
GetUtterancesView	Devuelve una vista de datos de enunciado totales para las versiones de un bot durante un periodo reciente	Enumeración	bot version*		
ListTagsForResource	Enumera las etiquetas de un recurso de Lex	Lectura	bot		
			bot alias		
			channel		
PostContent	Envía entradas de usuarios (texto o voz) a Amazon Lex	Escritura	bot alias		
			bot version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PostText	Envía entradas de usuarios (solo texto) a Amazon Lex	Escritura	bot alias		
			bot version		
PutBot	Crea o actualiza la versión $LATEST de un bot de conversación de Amazon Lex	Escritura	bot version*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutBotAlias	Crea o actualiza un alias para el bot específico	Escritura	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutIntent	Crea o actualiza la versión $LATEST de una intención	Escritura	intent version*		
PutSession	Crea una nueva sesión o modifica una sesión existente con un bot de Amazon Lex	Escritura	bot alias		
			bot version		
PutSlotType	Crea o actualiza la versión $LATEST de un tipo de ranura	Escritura	slottype version*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImport	Comienza un trabajo para importar un recurso a Amazon Lex	Escritura			
StartMigration	Otorga permiso para migrar un bot de Amazon Lex v1 a Amazon Lex v2	Escritura	bot version*		
TagResource	Agrega o sobrescribe etiquetas a un recurso de Lex	Etiquetado	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Elimina etiquetas de un recurso de Lex	Etiquetado	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	

Tipos de recurso definidos por Amazon Lex

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
bot	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}`	aws:ResourceTag/${TagKey}
bot version	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotVersion}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotAlias}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:lex:${Region}:${Account}:bot-channel:${BotName}:${BotAlias}:${ChannelName}`	aws:ResourceTag/${TagKey}
intent version	`arn:${Partition}:lex:${Region}:${Account}:intent:${IntentName}:${IntentVersion}`	
slottype version	`arn:${Partition}:lex:${Region}:${Account}:slottype:${SlotName}:${SlotVersion}`	

Claves de condición de Amazon Lex

Amazon Lex define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en

las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso en función de las etiquetas de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso Lex	Cadena
aws:TagKeys	Filtra el acceso en función del conjunto de claves de etiqueta en la solicitud	ArrayOfString
lex:associatedIntents	Permite controlar el acceso en función de las intenciones incluidas en la solicitud	ArrayOfString
lex:associatedSlotTypes	Permite controlar el acceso en función de los tipos de ranura incluidas en la solicitud	ArrayOfString
lex:channelType	Permite controlar el acceso en función del tipo de canal incluido en la solicitud	Cadena

Acciones, recursos y claves de condición para Amazon Lex V2

Amazon Lex V2 (prefijo de servicio: `lex`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de IAM permisos.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Lex V2
- Tipos de recursos definidos por Amazon Lex V2
- Claves de condición de Amazon Lex V2

Acciones definidas por Amazon Lex V2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchCreateCustomVocabularyItem	Otorga permiso para crear nuevos elementos en un vocabulario personalizado existente	Escritura	bot*		
BatchDeleteCustomVocabularyItem	Otorga permiso para eliminar elementos existentes de un vocabulario personalizado existente	Escritura	bot*		
BatchUpdateCustomVocabularyItem	Otorga permiso para actualizar los elementos existentes en un vocabulario personalizado existente	Escritura	bot*		
BuildBotLocale	Concede permiso para crear una configuración regional de bot existente en un bot	Write	bot*		
CreateBot	Concede permiso para crear un nuevo bot y un alias de bot	Write	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de prueba que apunte a la versión del bot DRAFT		bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotAlias	Concede permiso para crear un nuevo alias de bot en un bot	Write	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotChannel [solo permiso]	Concede permiso para crear un canal de bot en un bot existente	Write	bot*		
CreateBotLocale	Concede permiso para crear una nueva configuración regional de bot en un bot existente	Escritura	bot*		
CreateBotReplica	Concede permiso para crear réplicas de bot para un bot	Escritura	bot*		
CreateBotVersion	Concede permiso para crear una nueva versión de un bot existente	Escritura	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCustomVocabulary [solo permiso]	Concede permiso para crear un nuevo vocabulario personalizado en una configuración regional de bot existente	Escritura	bot*		
CreateExport	Concede permiso para crear una exportación para un recurso existente	Write	bot		
			test set		
CreateIntent	Concede permiso para crear una nueva intención en una configuración regional de bot existente	Write	bot*		
CreateResourcePolicy	Concede permiso para crear una nueva política de recursos para un recurso de Lex	Escritura	bot		
			bot alias		
CreateResourcePolicyStatement	Otorga permiso para crear una nueva declaración de política de recursos para un recurso de Lex	Escritura	bot		
			bot alias		
CreateSlot	Concede permiso para crear una nueva ranura en una intención	Write	bot*		
CreateSlotType	Concede permiso para crear un nuevo tipo de ranura en una configuración regional de bot existente	Escritura	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTestSet [solo permiso]	Concede permiso para importar un nuevo conjunto de pruebas	Escritura			
CreateTestSetDiscrepancyReport	Concede permiso para crear un informe de discrepancia de conjunto de pruebas	Escritura	test set*		
CreateUploadUrl	Concede permiso para crear una URL de carga para el archivo de importación	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBot	Concede permiso para eliminar un bot existente	Write	bot*		lex:DeleteBotAlias lex:DeleteBotChannel lex:DeleteBotLocale lex:DeleteBotVersion lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
			bot alias*		
DeleteBotAlias	Concede permiso para eliminar un alias de bot existente en un bot	Write	bot alias*		
DeleteBotChannel [solo permiso]	Concede permiso para eliminar un canal de bot existente	Write	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBotLocale	Concede permiso para eliminar una configuración regional de bot existente en un bot	Escritura	bot*		lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
DeleteBotReplica	Concede permiso para eliminar una réplica de bot existente	Escritura	bot*		
DeleteBotVersion	Concede permiso para eliminar una versión de bot existente.	Escritura	bot*		
DeleteCustomVocabulary	Concede permiso para eliminar un nuevo vocabulario personalizado en una configuración regional de bot existente	Escritura	bot*		
DeleteExport	Concede permiso para eliminar una exportación existente	Write	bot		
			test set		
DeleteImport	Concede permiso para eliminar una importación existente	Write	bot		
			test set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIntent	Concede permiso para eliminar una intención existente en una configuración regional de bot	Write	bot*		
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos existente para un recurso de Lex	Escritura	bot		
			bot alias		
DeleteResourcePolicyStatement	Otorga permiso para eliminar una declaración de política de recursos existente para un recurso de Lex	Escritura	bot		
			bot alias		
DeleteSession	Concede permiso para eliminar información de sesión para un alias de bot y un ID de usuario	Write	bot alias*		
DeleteSlot	Concede permiso para eliminar una ranura existente en una intención	Write	bot*		
DeleteSlotType	Concede permiso para eliminar un tipo de ranura existente en una configuración regional de bot	Escritura	bot*		
DeleteTestSet	Concede permiso para eliminar un conjunto de pruebas existente	Escritura	test set*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUtterances	Concede permiso para eliminar datos de enunciados de un bot	Escritura	bot*		
DescribeBot	Concede permiso para recuperar un bot existente	Read	bot*		
DescribeBotAlias	Concede permiso para recuperar un alias de bot existente	Read	bot alias*		
DescribeBotChannel [solo permiso]	Concede permiso para recuperar un canal de bot existente	Read	bot*		
DescribeBotLocale	Concede permiso para recuperar una configuración regional de bot existente	Lectura	bot*		
DescribeBotRecommendation	Concede permiso para recuperar información de metadatos sobre una recomendación de bot.	Lectura	bot*		
DescribeBotReplica	Concede permiso para obtener una réplica de bot existente	Lectura	bot*		
DescribeBotResourceGeneration	Concede permiso para recuperar información de metadatos para la generación de recursos de bot	Lectura	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBotVersion	Concede permiso para recuperar una versión de bot existente.	Lectura	bot*		
DescribeCustomVocabulary [solo permiso]	Concede permiso para recuperar un vocabulario personalizado existente	Lectura	bot*		
DescribeCustomVocabularyMetadata	Concede permiso para recuperar los metadatos de un vocabulario personalizado existente	Lectura	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeExport	Concede permiso para recuperar una exportación existente	Read	bot		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex:ListBotLocales lex:ListIntents lex:ListSlotTypes lex:ListSlots
			test set		
DescribeImport	Concede permiso para recuperar una importación existente	Read	bot		
			test set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeIntent	Concede permiso para recuperar una intención existente	Read	bot*		
DescribeResourcePolicy	Concede permiso para recuperar una política de recursos existente para un recurso de Lex	Read	bot		
			bot alias		
DescribeSlot	Concede permiso para recuperar una ranura existente	Read	bot*		
DescribeSlotType	Concede permiso para recuperar un tipo de ranura existente	Lectura	bot*		
DescribeTestExecution	Concede permiso para recuperar los metadatos de ejecución de una prueba	Lectura	test set*		
DescribeTestSet	Concede permiso para recuperar un conjunto de pruebas existente	Lectura	test set*		
DescribeTestSetDiscrepancyReport	Concede permiso para recuperar los metadatos del informe de discrepancias del conjunto de pruebas	Lectura	test set*		
DescribeTestSetGeneration	Concede permiso para recuperar los metadatos de generación del conjunto de pruebas	Lectura	test set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateBotElement	Concede permiso para generar campos o elementos compatibles para un bot	Lectura	bot*		
GetSession	Concede permiso para recuperar información de sesión para un alias de bot y un ID de usuario.	Lectura	bot alias*		
GetTestExecutionArtifactsUrl	Concede permiso para recuperar la URL de los artefactos para la ejecución de una prueba	Lectura	test set*		
ListAggregatedUtterances	Concede permiso para enumerar las declaraciones y estadísticas de un bot.	Enumeración	bot*		
ListBotAliasReplicas	Concede permiso para enumerar réplicas de alias en una réplica de bot	Enumeración	bot*		
ListBotAliases	Concede permiso para enumerar alias de bot en un bot	List	bot*		
ListBotChannels [solo permiso]	Concede permiso para enumerar canales de bot	List	bot*		
ListBotLocales	Concede permiso para enumerar configuraciones regionales de bot en un bot	Enumeración	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBotRecommendations	Concede permiso para obtener una lista de recomendaciones de bot que cumplen los criterios especificados.	Enumeración	bot*		
ListBotReplicas	Concede permiso para enumerar réplicas de un bot	Enumeración	bot*		
ListBotResourceGenerations	Concede permiso para enumerar las generaciones de recursos de un bot	Enumeración	bot*		
ListBotVersionReplicas	Concede permiso para enumerar réplicas de versiones en una réplica de bot	Enumeración	bot*		
ListBotVersions	Concede permiso para enumerar versiones de bot existentes	List	bot*		
ListBots	Concede permiso para enumerar bots existentes	List			
ListBuiltInIntents	Concede permiso para enumerar intenciones integradas	List			
ListBuiltInSlotTypes	Concede permiso para enumerar tipos de ranuras integradas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCustomVocabularyItems	Otorga permiso para enumerar elementos de un vocabulario personalizado existente	Enumeración	bot*		
ListExports	Concede permiso para enumerar exportaciones existentes	List			
ListImports	Concede permiso para enumerar importaciones existentes	Enumeración			
ListIntentMetrics	Otorga permiso para enumerar métricas de análisis de intención para un bot	Enumeración	bot*		
ListIntentPaths	Otorga permiso para enumerar análisis de ruta de intención para un bot	Enumeración	bot*		
ListIntentStageMetrics	Otorga permiso para enumerar las métricas de análisis de intentStage para un bot	Enumeración	bot*		
ListIntents	Concede permiso para enumerar intenciones en un bot	Enumeración	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRecommendedIntents	Concede permiso para obtener una lista de intenciones recomendadas proporcionadas por la recomendación del bot.	Enumeración	bot*		
ListSessionAnalyticsData	Otorga permiso para enumerar datos de análisis de sesión para un bot	Enumeración	bot*		
ListSessionMetrics	Otorga permiso para enumerar las métricas de análisis de sesión para un bot	Enumeración	bot*		
ListSlotTypes	Concede permiso para enumerar tipos de ranuras en un bot	List	bot*		
ListSlots	Concede permiso para enumerar ranuras en una intención	List	bot*		
ListTagsForResource	Concede permiso a listas de etiquetas para un recurso Lex	Lectura	bot		
			bot alias		
			test set		
ListTestExecutionResultItems	Concede permiso para recuperar los datos de los resultados de la prueba para la ejecución de una prueba	Lectura	test set*		lex:ListTestSetRecords

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTestExecutions	Concede permiso para enumerar las ejecuciones de prueba	Enumeración			
ListTestSetRecords	Concede permiso para recuperar los registros contenidos en un conjunto de pruebas existente	Lectura	test set*		
ListTestSets	Concede permiso para enumerar conjuntos de pruebas	Enumeración			
PutSession	Concede permiso para crear una nueva sesión o modificar una sesión existente para un alias de bot y un ID de usuario	Escritura	bot alias*		
RecognizeText	Concede permiso para enviar la entrada del usuario (sólo texto) a un alias de bot	Escritura	bot alias*		
RecognizeUtterance	Concede permiso para enviar la entrada del usuario (texto o voz) a un alias de bot	Escritura	bot alias*		
SearchAssociatedTranscripts	Concede permiso para buscar transcripciones asociadas que cumplan los criterios especificados.	Enumeración	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartBotRecommendation	Concede permiso para iniciar una recomendación de bot para una configuración regional de bot.	Escritura	bot*		
StartBotResourceGeneration	Concede permiso para iniciar una generación de recursos para una configuración regional de bot	Escritura	bot*		
StartConversation	Otorga permiso para transmitir la entrada del usuario (speech/text/DTMF) a un alias de bot	Escritura	bot alias*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImport	Concede permiso para iniciar una nueva importación con el archivo de importación cargado	Escritura	bot		lex:CreateBot lex:CreateBotLocale lex:CreateCustomVocabulary lex:CreateIntent lex:CreateSlot lex:CreateSlotType lex:CreateTestSet lex:DeleteBotLocale lex:DeleteCustomVocabulary lex:DeleteIntent

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					lex:DeleteSlot lex:DeleteSlotType lex:UpdateBot lex:UpdateBotLocale lex:UpdateCustomVocabulary lex:UpdateIntent lex:UpdateSlot lex:UpdateSlotType lex:UpdateTestSet
			bot alias		
			test set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
StartTestExecution	Concede permiso para iniciar la ejecución de una prueba mediante un conjunto de pruebas	Escritura	test set*		
StartTestSetGeneration	Concede permiso para generar un conjunto de pruebas	Escritura	test set		
StopBotRecommendation	Concede permiso para detener una recomendación de bot para una configuración regional de bot.	Escritura	bot*		
TagResource	Concede permiso para agregar o sobrescribir etiquetas de un recurso Lex	Etiquetado	bot		
			bot alias		
			test set		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas de un recurso Lex	Etiquetado	bot		
			bot alias		
			test set		
				aws:TagKeys	
UpdateBot	Concede permiso para actualizar un bot existente	Write	bot*		
UpdateBotAlias	Concede permiso para actualizar un alias de bot existente	Write	bot alias*		
UpdateBotLocale	Concede permiso para actualizar un bot regional existente	Escritura	bot*		
UpdateBotRecommendation	Concede permiso para actualizar una solicitud de recomendación de bot existente.	Escritura	bot*		
UpdateCustomVocabulary [solo permiso]	Concede permiso para actualizar un vocabulario personalizado existente	Escritura	bot*		
UpdateExport	Concede permiso para actualizar una exportación existente	Write	bot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIntent	Concede permiso para actualizar una intención existente	Write	bot*		
UpdateResourcePolicy	Concede permiso para actualizar una política de recursos existente para un recurso de Lex	Write	bot		
			bot alias		
UpdateSlot	Concede permiso para actualizar una ranura existente	Write	bot*		
UpdateSlotType	Concede permiso para actualizar un tipo de ranura existente	Escritura	bot*		
UpdateTestSet	Concede permiso para actualizar un conjunto de pruebas existente	Escritura	test set*		

Tipos de recursos definidos por Amazon Lex V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
bot	`arn:${Partition}:lex:${Region}:${Account}:bot/${BotId}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot-alias/${BotId}/${BotAliasId}`	aws:ResourceTag/${TagKey}
test set	`arn:${Partition}:lex:${Region}:${Account}:test-set/${TestSetId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Lex V2

Amazon Lex V2 define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una IAM política. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso Lex	Cadena
aws:TagKeys	Filtra el acceso mediante el conjunto de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS License Manager

AWS License Manager (prefijo de servicio:`license-manager`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS License Manager
- Tipos de recursos definidos por AWS License Manager
- Claves de condición para AWS License Manager

Acciones definidas por AWS License Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptGrant	Otorga permiso para aceptar una concesión.	Write	grant*		
CheckInLicense	Otorga permiso para devolver concesiones de derechos de licencia al grupo.	Write			
CheckoutBorrowLicense	Otorga permiso para comprobar concesiones de	Write	license*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	derechos de licencia para el caso de uso de préstamo.				
CheckoutLicense	Otorga permiso para comprobar concesiones de derechos de licencia.	Write			
CreateGrant	Otorga permiso para crear una nueva concesión de licencia.	Write	license*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGrantVersion	Otorga permiso para crear una nueva versión de concesión.	Write	grant*		
CreateLicense	Otorga permiso para crear una nueva licencia.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConfiguration	Otorga permiso para crear una nueva configuración de licencia.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLicenseConversionTaskForResource	Otorga permiso para crear una tarea de conversión de licencia para un recurso	Escritura			
CreateLicenseManagerReportGenerator	Otorga permiso para crear un generador de informes para una configuración de licencia	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	Otorga permiso para crear una nueva versión de licencia	Escritura	license*		
CreateToken	Otorga permiso para crear un nuevo token para la licencia.	Escritura	license*		
DeleteGrant	Otorga permiso para eliminar una concesión	Escritura	grant*		
DeleteLicense	Otorga permiso para eliminar una licencia.	Write	license*		
DeleteLicenseConfiguration	Otorga permiso para eliminar permanentemente una configuración de licencia.	Write	license-configuration*		
DeleteLicenseManagerReportGenerator	Otorga permiso para eliminar un generador de informes	Write	report-generator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteToken	Otorga permiso para eliminar el token.	Write			
ExtendLicenseConsumption	Otorga permiso para extender el periodo de consumo de las concesiones de derechos de licencia ya comprobadas.	Write			
GetAccessToken	Otorga permiso para obtener el token de acceso.	Read			
GetGrant	Otorga permiso para obtener una concesión.	Read	grant*		
GetLicense	Otorga permiso para obtener una licencia.	Read	license*		
GetLicenseConfiguration	Otorga permiso para obtener una configuración de licencia.	Lectura	license-configuration*		
GetLicenseConversionTask	Otorga permiso para recuperar una tarea de conversión de licencia	Lectura			
GetLicenseManagerReportGenerator	Otorga permiso para obtener un generador de informes	Read	report-generator*		
GetLicenseUsage	Otorga permiso para obtener el uso de licencias.	Read	license*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceSettings	Otorga permiso para obtener una configuración de servicio.	List			
ListAssociationsForLicenseConfiguration	Otorga permiso para enumerar las asociaciones para una configuración de licencia selecta.	List	license-configuration*		
ListDistributedGrants	Otorga permiso para enumerar las concesiones distribuidas.	List			
ListFailuresForLicenseConfigurationOperations	Otorga permiso para enumerar las operaciones de configuración de licencias que tuvieron errores.	List	license-configuration*		
ListLicenseConfigurations	Otorga permiso para enumerar las configuraciones de licencia.	Lectura			
ListLicenseConversionTasks	Otorga permiso para enumerar las tareas de conversión de licencia	Enumeración			
ListLicenseManagerReportGenerators	Otorga permiso para enumerar generadores de informes	List	license-configuration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLicenseSpecificationsForResource	Otorga permiso para enumerar las especificaciones de licencia asociadas a un recurso selecto.	List			
ListLicenseVersions	Otorga permiso para enumerar las versiones de licencia.	List	license*		
ListLicenses	Otorga permiso para enumerar las licencias.	Lectura			
ListReceivedGrants	Otorga permiso para enumerar las concesiones recibidas.	Enumeración			
ListReceivedGrantsForOrganization	Otorga permiso para enumerar las concesiones recibidas para la organización	Enumeración			
ListReceivedLicenses	Otorga permiso para enumerar las licencias recibidas.	Enumeración			
ListReceivedLicensesForOrganization	Otorga permiso para enumerar las licencias recibidas para la organización	Enumeración			
ListResourceInventory	Otorga permiso para enumerar el inventario de recursos.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para enumerar las etiquetas para un recurso selecto.	Lectura	grant		
			license		
			license-configuration		
			report-generator		
ListTokens	Otorga permiso para enumerar los tokens.	List			
ListUsageForLicenseConfiguration	Otorga permiso para enumerar los registros de uso para la configuración de licencia selecta.	List	license-configuration*		
RejectGrant	Otorga permiso para rechazar una concesión.	Write	grant*		
TagResource	Otorga permiso para etiquetar un recurso selecto.	Etiquetado	grant		
			license		
			license-configuration		
			report-generator		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar la etiqueta de un recurso selecto.	Etiquetado	grant		
			license		
			license-configuration		
			report-generator		
				aws:TagKeys	
UpdateLicenseConfiguration	Otorga permiso para actualizar una configuración de licencia existente.	Write	license-configuration*		
UpdateLicenseManagerReportGenerator	Otorga permiso para actualizar un generador de informes para una configuración de licencia	Write	report-generator*		
UpdateLicenseSpecificationsForResource	Otorga permiso para actualizar las especificaciones de licencia para un recurso selecto.	Write	license-configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceSettings	Otorga permiso para actualizar una configuración de servicio.	Permissions management			

Tipos de recursos definidos por AWS License Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
license-configuration	`arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}`	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}
license	`arn:${Partition}:license-manager::${Account}:license:${LicenseId}`	aws:ResourceTag/${TagKey}
grant	`arn:${Partition}:license-manager::${Account}:grant:${GrantId}`	aws:ResourceTag/${TagKey}
report-generator	`arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
		license-manager:ResourceTag/${TagKey}

Claves de condición para AWS License Manager

AWS License Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
license-manager:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena

Acciones, recursos y claves de condición para AWS License Manager Linux Subscriptions Manager

AWS License Manager Linux Subscriptions Manager (prefijo de servicio:`license-manager-linux-subscriptions`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS License Manager Linux Subscriptions Manager
- Tipos de recursos definidos por AWS License Manager Linux Subscriptions Manager
- Claves de condición para AWS License Manager Linux Subscriptions Manager

Acciones definidas por AWS License Manager Linux Subscriptions Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterSubscriptionProvider	Otorga permiso para eliminar permanentemente un proveedor de suscripciones en AWS License Manager	Escritura	subscription-provider*		
GetRegisteredSubscriptionProvider	Otorga permiso para obtener un proveedor de suscripciones en AWS License Manager	Lectura	subscription-provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceSettings	Otorga permiso para obtener la configuración del servicio para las suscripciones de Linux en AWS License Manager	Lectura			
ListLinuxSubscriptionInstances	Otorga permiso para enumerar todas las instancias con suscripciones de Linux en AWS License Manager	Lectura			
ListLinuxSubscriptions	Otorga permiso para enumerar todas las suscripciones de Linux en AWS License Manager	Lectura			
ListRegisteredSubscriptionProviders	Otorga permiso para incluir proveedores de suscripciones en AWS License Manager	Lectura			
ListTagsForResource	Otorga permiso para enumerar las etiquetas para un recurso selecto.	Lectura	subscription-provider*		
RegisterSubscriptionProvider	Otorga permiso para crear un nuevo proveedor de suscripciones en AWS License Manager	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar un recurso selecto.	Etiquetado	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar la etiqueta de un recurso selecto.	Etiquetado	subscription-provider*		
				aws:TagKeys	
UpdateServiceSettings	Otorga permiso para actualizar la configuración del servicio para las suscripciones de Linux en AWS License Manager	Escritura			

Tipos de recursos definidos por AWS License Manager Linux Subscriptions Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
subscription-provider	`arn:${Partition}:license-manager-linux-subscriptions:${Region}:${Account}:subscription-provider/${SubscriptionProviderId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS License Manager Linux Subscriptions Manager

AWS License Manager Linux Subscriptions Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS License Manager User Subscriptions

AWS Las suscripciones de usuario de License Manager (prefijo de servicio:`license-manager-user-subscriptions`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS License Manager User Subscriptions
- Tipos de recursos definidos por AWS License Manager User Subscriptions
- Claves de condición para AWS License Manager User Subscriptions

Acciones definidas por AWS License Manager User Subscriptions

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate User	Concede permiso para asociar un usuario suscrito a una instancia lanzada con productos de License Manager User Subscriptions	Escritura	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLicenseServerEndpoint	Otorga permiso para crear un punto final de servidor de licencias para un tipo de servidor determinado y para un proveedor de identidad determinado	Escritura	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLicenseServerEndpoint	Otorga permiso para eliminar un punto final del servidor de licencias para un tipo de servidor determinado para un proveedor de identidad determinado	Escritura	identity-provider*		
			license-server-endpoint*		
DeregisterIdentityProvider	Otorga permiso para anular el registro de Microsoft Active Directory en un license-manager-user-subscriptions producto	Escritura	identity-provider*		
DisassociateUser	Concede permiso para desasociar a un usuario suscrito de una instancia lanzada con productos de License Manager User Subscriptions	Escritura	identity-provider*		
			instance-user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIdentityProviders	Otorga permiso para enumerar todos los proveedores de identidad en las suscripciones de usuario del administrador de licencias	Enumeración			
ListInstances	Concede permiso para enumerar todas las instancias lanzadas con productos de License Manager User Subscriptions	Enumeración			
ListLicenseServerEndpoints	Otorga permiso para enumerar los puntos finales del servidor de licencias	Enumeración			
ListProductSubscriptions	Concede permiso para enumerar todas las suscripciones de productos de un proveedor de productos e identidades	Enumeración	identity-provider*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas para un recurso selecto.	Lectura	identity-provider*		
			instance-user*		
			license-server-endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			product-subscription*		
ListUserAssociations	Concede permiso para enumerar todos los usuarios asociados a una instancia lanzada para un producto	Enumeración	identity-provider*		
RegisterIdentityProvider	Otorga permiso para registrar Microsoft Active Directory license-manager-user-subscriptions para un producto	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
StartProductSubscription	Concede permiso para iniciar la suscripción de un producto a un usuario en un directorio activo registrado para un producto	Escritura	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopProductSubscription	Concede permiso para detener la suscripción de un producto a un usuario en un directorio activo registrado para un producto	Escritura	identity-provider*		
			product-subscription*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar un recurso selecto.	Etiquetado	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar la etiqueta de un recurso selecto.	Etiquetado	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIdentityProviderSettings	Otorga permiso para actualizar la configuración del proveedor de identidades	Escritura	identity-provider*		

Tipos de recursos definidos por AWS License Manager User Subscriptions

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
identity-provider	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:identity-provider/${IdentityProviderId}`	aws:ResourceTag/${TagKey}
product-subscription	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:product-subscription/${ProductSubscriptionId}`	aws:ResourceTag/${TagKey}
instance-user	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:instance-user/${InstanceUserId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
license-server-endpoint	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:license-server-endpoint/${LicenseServerEndpointId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS License Manager User Subscriptions

AWS License Manager User Subscriptions define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Lightsail

Amazon Lightsail (prefijo de servicio: `lightsail`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Lightsail
- Tipos de recurso definidos por Amazon Lightsail
- Claves de condición de Amazon Lightsail

Acciones definidas por Amazon Lightsail

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllocateStaticIp	Otorga permiso para crear una dirección IP estática que se puede asociar a una instancia	Escritura			
AttachCertificateToDistribution	Otorga permiso para adjuntar un SSL/TLS certificado a su distribución en la red de entrega de contenido (CDN) de Amazon Lightsail	Escritura	Certificate*		
			Distribution*		
AttachDisk	Otorga permiso para asociar un disco a una instancia	Write	Disk*		
AttachInstancesToLoadBalancer	Otorga permiso para asociar una o varias instancias a un balanceador de carga	Write	LoadBalancer*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AttachLoadBalancerTlsCertificate	Otorga permiso para asociar un certificado TLS a un balanceador de carga	Write	LoadBalancer*		
AttachStaticIp	Otorga permiso para asociar una dirección IP estática a una instancia	Write	Instance*		
			StaticIp*		
CloseInstancePublicPorts	Otorga permiso para cerrar un puerto público de una instancia	Escritura	Instance*		
CopySnapshot	Otorga permiso para copiar una instantánea de una Región de AWS a otra en Amazon Lightsail	Escritura			
CreateBucket	Otorga permiso para crear un bucket de Amazon Lightsail	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBucketAccessKey	Otorga permiso para crear una clave de acceso nueva para el bucket especificado	Escritura	Bucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCertificate	Otorga permiso para crear un certificado SSL/TLS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateCloudFormationStack	Concede permiso para crear una nueva EC2 instancia de Amazon a partir de una instantánea exportada de Amazon Lightsail	Escritura			
CreateContactMethod	Otorga permiso para crear un método de contacto de mensaje de texto o email	Write			
CreateContainerService	Otorga permiso para crear un servicio de contenedores de Amazon Lightsail	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContainerServiceDeployment	Otorga permiso para crear una implementación para su servicio de contenedores de Amazon Lightsail	Write	ContainerService*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateContainerServiceRegistryLogin	Otorga permiso para crear un conjunto temporal de credenciales de inicio de sesión que puede utilizar a fin de iniciar sesión en el proceso Docker en su equipo local	Write			
CreateDisk	Otorga permiso para crear un disco	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskFromSnapshot	Otorga permiso para crear un disco a partir de instantáneas	Write	DiskSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskSnapshot	Otorga permiso para crear una instantánea de disco	Write	Disk		
			Instance		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDistribution	Otorga permiso para crear una distribución de red de entrega de contenido (CDN) de Amazon Lightsail	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDomain	Otorga permiso para crear un recurso de dominio para el nombre de dominio especificado	Write		aws:RequestTag/${TagKey} aws:TagKeys	route53:DeleteHostedZone route53:GetHostedZone route53:ListHostedZonesByName route53domains:GetDomainDetail route53domains:GetOperationDetail route53domains:ListDomains route53domains:ListOperations route53domains:Upd

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ateDomainNameservers
CreateDomainEntry	Otorga permiso para crear una o varias entradas de registro de DNS para un recurso de dominio: dirección (A), nombre canónico (CNAME), intercambio de correo (MX), servidor de nombres (NS), inicio de autoridad (SOA), localizador de servicios (SRV) o texto (TXT)	Escritura	Domain*		
CreateGUISessionAccessDetails	Otorga permisos de creación URLs que se utilizan para acceder a la sesión de interfaz gráfica de usuario (GUI) de una instancia	Escritura	Instance*		
CreateInstanceSnapshot	Otorga permiso para crear una instantánea de la instancia	Write	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInstances	Otorga permiso para crear una o varias instancias	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstancesFromSnapshot	Otorga permiso para crear una o varias instancias a partir de una instantánea de instancia	Write	InstanceSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeyPair	Otorga permiso para crear un par de claves que se utiliza para autenticar una instancia y conectarse a ella	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoadBalancer	Concede permiso para crear un balanceador de carga	Write		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLoadBalancerTlsCertificate	Otorga permiso para crear un certificado TLS de balanceador de carga	Write	LoadBalancer*		lightsail:CreateDomainEntry lightsail:GetDomains
CreateRelationalDatabase	Otorga permiso para crear una nueva base de datos relacional	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseFromSnapshot	Otorga permiso para crear una nueva base de datos relacional a partir de una instantánea	Write	RelationalDatabaseSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseSnapshot	Otorga permiso para crear una instantánea de base de datos relacional	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAlarm	Otorga permiso para eliminar una alarma	Write	Alarm*		
DeleteAutoSnapshot	Otorga permiso para eliminar una instantánea automática de una instancia o disco	Write			
DeleteBucket	Otorga permiso para eliminar un bucket de Amazon Lightsail	Write	Bucket*		
DeleteBucketAccessKey	Otorga permiso para eliminar una clave de acceso para un bucket de Amazon Lightsail especificado	Escritura	Bucket*		
DeleteCertificate	Otorga permiso para eliminar un SSL/TLS certificado	Escritura	Certificate*		
DeleteContactMethod	Otorga permiso para eliminar un método de contacto	Write			
DeleteContainerImage	Otorga permiso para eliminar una imagen de contenedor registrada en su servicio de contenedores de Amazon Lightsail	Write	ContainerService*		
DeleteContainerService	Otorga permiso para eliminar el servicio de contenedores de Amazon Lightsail	Write	ContainerService*		
DeleteDisk	Otorga permiso para eliminar un disco	Write	Disk*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDiskSnapshot	Otorga permiso para eliminar una instantánea de disco	Write	DiskSnapshot*		
DeleteDistribution	Otorga permiso para eliminar la distribución de la red de entrega de contenido (CDN) de Amazon Lightsail	Write	Distribution*		
DeleteDomain	Otorga permiso para eliminar un recurso de dominio y todos sus registros de DNS	Write	Domain*		
DeleteDomainEntry	Otorga permiso para eliminar una entrada de registro de DNS para un recurso de dominio	Write	Domain*		
DeleteInstance	Otorga permiso para eliminar una instancia	Write	Instance*		
DeleteInstanceSnapshot	Otorga permiso para eliminar una instantánea de instancia	Write	InstanceSnapshot*		
DeleteKeyPair	Otorga permiso para eliminar un par de claves que se utiliza para autenticar una instancia y conectarse a ella	Write	KeyPair*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteKnownHostKeys	Otorga permiso para eliminar el certificado o clave de host conocido que usan los clientes SSH o RDP basados en el navegador de Amazon Lightsail para autenticar una instancia	Write	Instance*		
DeleteLoadBalancer	Otorga permiso para eliminar un balanceador de carga	Write	LoadBalancer*		
DeleteLoadBalancerTlsCertificate	Otorga permiso para eliminar un certificado TLS de balanceador de carga	Write	LoadBalancer*		
DeleteRelationalDatabase	Otorga permiso para eliminar una base de datos relacional	Write	RelationalDatabase*		
DeleteRelationalDatabaseSnapshot	Otorga permiso para eliminar una instantánea de base de datos relacional	Escritura	RelationalDatabaseSnapshot*		
DetachCertificateFromDistribution	Otorga permiso para separar un SSL/TLS certificado de su distribución en la red de entrega de contenido (CDN) de Amazon Lightsail	Escritura	Distribution*		
DetachDisk	Otorga permiso para desconectar un disco de una instancia	Write	Disk*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetachInstancesFromLoadBalancer	Otorga permiso para desconectar una o varias instancias de un balanceador de carga	Write	LoadBalancer*		
DetachStaticIp	Otorga permiso para desconectar una IP estática de una instancia a la que está asociada	Write	StaticIp*		
DisableAddOn	Otorga permiso para desactivar un complemento para un recurso de Amazon Lightsail	Escritura			
DownloadDefaultKeyPair	Otorga permiso para descargar el key pair predeterminado que se usa para autenticar y conectarse a instancias en un entorno específico Región de AWS	Escritura			
EnableAddOn	Otorga permiso para habilitar o modificar un complemento para un recurso de Amazon Lightsail	Escritura			
ExportSnapshot	Concede permiso para exportar una instantánea de Amazon Lightsail a Amazon EC2	Escritura	DiskSnapshot		iam:CreateServiceLinkedRole iam:PutRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			InstanceSnapshot		
GetActiveNames	Otorga permiso para obtener los nombres de todos los recursos activos (no eliminados)	Read			
GetAlarms	Otorga permiso para ver información sobre las alarmas configuradas	Read			
GetAutoSnapshots	Otorga permiso para ver las instantáneas automáticas disponibles para una instancia o disco	Read			
GetBlueprints	Otorga permiso para obtener una lista de imágenes de instancia o proyectos Puede utilizar un proyecto para crear una instancia nueva que ya esté ejecutando un sistema operativo específico, así como una aplicación preinstalada o una pila de desarrollo. El software que se ejecuta en la instancia depende del proyecto que defina al crear la instancia	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBucketAccessKeys	Otorga permiso para obtener la clave de acceso existente IDs para el bucket de Amazon Lightsail especificado	Lectura			
GetBucketBundles	Otorga permiso para obtener los paquetes que se pueden aplicar a un bucket de Amazon Lightsail	Read			
GetBucketMetricData	Otorga permiso para obtener los puntos de datos de una métrica específica para un bucket de Amazon Lightsail	Read			
GetBuckets	Otorga permiso para obtener información sobre uno o varios buckets de Amazon Lightsail	Read			
GetBundles	Otorga permiso para obtener una lista de paquetes de instancias. Puede utilizar un paquete para crear una nueva instancia con un conjunto de especificaciones de rendimiento, como el recuento de CPU, el tamaño del disco, el tamaño de RAM y el límite de transferencia de red. El costo de la instancia depende del paquete que defina al crear la instancia	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCertificates	Otorga permiso para ver información sobre uno o más certificados de Amazon Lightsail SSL/TLS	Lectura			
GetCloudFormationStackRecords	Otorga permiso para obtener información sobre todas las CloudFormation pilas utilizadas para crear EC2 recursos de Amazon a partir de instantáneas exportadas de Amazon Lightsail	Lectura			
GetContactMethods	Otorga permiso para ver información sobre los métodos de contacto configurados	Read			
GetContainerAPIMetadata	Otorga permiso para ver información sobre los contenedores de Amazon Lightsail, como la versión actual del complemento de Lightsail Control (lightsailctl)	Read			
GetContainerImages	Otorga permiso para ver las imágenes de contenedor registradas en su servicio de contenedores de Amazon Lightsail	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetContainerLog	Otorga permiso para ver los eventos de registro de un contenedor de su servicio de contenedores de Amazon Lightsail	Read			
GetContainerServiceDeployments	Otorga permiso para ver las implementaciones de su servicio de contenedores de Amazon Lightsail	Read			
GetContainerServiceMetricData	Otorga permiso para ver los puntos de datos de una métrica específica de su servicio de contenedores de Amazon Lightsail	Read			
GetContainerServicePowers	Otorga permiso para ver la lista de facultades que se pueden especificar para sus servicios de contenedores de Amazon Lightsail	Read			
GetContainerServices	Otorga permiso para ver información sobre uno o varios de sus servicios de contenedores de Amazon Lightsail	Lectura			
GetCostEstimate	Concede permiso para obtener información sobre la estimación de costo de un recurso especificado	Lectura	Disk Instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDisk	Otorga permiso para obtener información sobre un disco	Read			
GetDiskSnapshot	Otorga permiso para obtener información sobre una instantánea de disco	Read			
GetDiskSnapshots	Otorga permiso para obtener información sobre todas las instantáneas de disco	Read			
GetDisks	Otorga permiso para obtener información sobre todos los discos	Read			
GetDistributionBundles	Otorga permiso para ver la lista de paquetes que se pueden aplicar a las distribuciones de la red de entrega de contenido (CDN) de Amazon Lightsail	Read			
GetDistributionLatestCacheReset	Otorga permiso para ver la marca de tiempo y el estado del último restablecimiento de caché de una distribución específica de la red de entrega de contenido (CDN) de Amazon Lightsail	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDistributionMetricData	Otorga permiso para ver los puntos de datos de una métrica específica para una distribución de la red de entrega de contenido (CDN) de Amazon Lightsail	Read			
GetDistributions	Otorga permiso para ver información sobre una o más de sus distribuciones de la red de entrega de contenido (CDN) de Amazon Lightsail	Read			
GetDomain	Otorga permiso para obtener un registro de DNS para un recurso de dominio	Read			
GetDomains	Otorga permiso para obtener registros de DNS para todos los recursos de dominio	Lectura			
GetExportSnapshotRecords	Concede permiso para obtener información sobre todos los registros de las instantáneas de Amazon Lightsail exportadas a Amazon EC2	Lectura			
GetInstance	Otorga permiso para obtener información acerca de una instancia	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetInstanceAccessDetails	Otorga permiso para obtener claves temporales que usted puede utilizar para autenticar y conectarse a una instancia	Write	Instance*		
GetInstanceMetricData	Otorga permiso para obtener los puntos de datos de la métrica especificada de una instancia	Read			
GetInstancePortStates	Otorga permiso para obtener los estados de puerto de una instancia	Read			
GetInstanceSnapshot	Otorga permiso para obtener información acerca de una instantánea de instancia	Read			
GetInstanceSnapshots	Otorga permiso para obtener información acerca de todas las instantáneas de instancia	Read			
GetInstanceState	Otorga permiso para obtener el estado de una instancia	Read			
GetInstances	Otorga permiso para obtener información acerca de todas las instancias	Read			
GetKeyPair	Otorga permiso para obtener información sobre un par de claves	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetKeyPairs	Otorga permiso para obtener información sobre todos los pares de claves	Lectura			
GetLoadBalancer	Otorga permiso para obtener información sobre un equilibrador de carga	Lectura			
GetLoadBalancerMetricData	Otorga permiso para obtener los puntos de datos de la métrica especificada de un balanceador de carga	Read			
GetLoadBalancerTlsCertificates	Otorga permiso para obtener información sobre un certificado de TLS del balanceador de carga	Lectura			
GetLoadBalancerTlsPolicies	Otorga permiso para obtener una lista de las políticas de seguridad TLS que puede aplicar a los equilibradores de carga de Lightsail	Lectura			
GetLoadBalancers	Otorga permiso para obtener información sobre balanceadores de carga	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOperation	Otorga permiso para obtener información acerca de una operación Las operaciones incluyen eventos como cuándo crear una instancia, asignar una IP estática, asociar una IP estática y así sucesivamente	Read			
GetOperations	Otorga permiso para obtener información acerca de todas las operaciones Las operaciones incluyen eventos como cuándo crear una instancia, asignar una IP estática, asociar una IP estática y así sucesivamente	Read			
GetOperationsForResource	Otorga permiso para obtener operaciones de un recurso	Lectura			
GetRegions	Otorga permiso para obtener una lista de todos los productos válidos Regiones de AWS para Amazon Lightsail	Lectura			
GetRelationalDatabase	Otorga permiso para obtener información sobre una base de datos relacional	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRelationalDatabaseBlueprints	Otorga permiso para obtener una lista de imágenes de base de datos relacional o proyectos Puede utilizar un proyecto para crear una nueva base de datos que ejecute un motor de base de datos específico. El motor de base de datos que se ejecuta en la base de datos depende del proyecto que defina al crear la base de datos relacional	Read			
GetRelationalDatabaseBundles	Otorga permiso para obtener una lista de paquetes de base de datos relacional Puede utilizar un paquete para crear una nueva base de datos con un conjunto de especific aciones de rendimiento, como el recuento de CPU, el tamaño del disco, el tamaño de RAM, el límite de transferencia de red y el estándar de alta disponibilidad. El costo de la base de datos depende del paquete que defina al crear la base de datos relacional	Read			
GetRelationalDatabaseEvents	Otorga permiso para obtener eventos para una base de datos relacional	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRelationalDatabaseLogEvents	Otorga permiso para obtener eventos para el flujo de registros especificado de una base de datos relacional	Read			
GetRelationalDatabaseLogStreams	Otorga permiso para obtener flujos de registros disponibles para una base de datos relacional	Read			
GetRelationalDatabaseMasterUserPassword	Otorga permiso para obtener la contraseña de usuario maestro de una base de datos relacional	Write	RelationalDatabase*		
GetRelationalDatabaseMetricData	Otorga permiso para obtener los puntos de datos de la métrica especificada de una base de datos relacional	Read			
GetRelationalDatabaseParameters	Otorga permiso para obtener los parámetros de una base de datos relacional	Read			
GetRelationalDatabaseSnapshot	Otorga permiso para obtener información sobre una instantánea de base de datos relacional	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRelationalDatabaseSnapshots	Otorga permiso para obtener información sobre todas las instantáneas de base de datos relacional	Read			
GetRelationalDatabases	Otorga permiso para obtener información sobre todas las bases de datos relacionales	Lectura			
GetSetupHistory	Concede permiso para obtener información detallada de las solicitudes de configuración ejecutadas en el recurso especificado	Lectura	Instance		
GetStaticIp	Otorga permiso para obtener información sobre una IP estática	Lectura			
GetStaticIps	Otorga permiso para obtener información sobre todas las estadísticas IPs	Lectura			
ImportKeyPair	Otorga permiso para importar una clave pública desde un par de claves	Write			
IsVpcPeered	Otorga permiso para obtener un valor booleano que indica si la Virtual Private Cloud (VPC) de Amazon Lightsail está interconectada	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
OpenInstancePublicPorts	Otorga permiso para agregar o abrir un puerto público de una instancia	Write	Instance*		
PeerVpc	Otorga permiso para tratar de interconectar la Virtual Private Cloud (VPC) de Amazon Lightsail con la VPC predeterminada	Write			
PutAlarm	Otorga permiso para crear o actualizar una alarma y asociarla con la métrica especificada	Write	Alarm*		
PutInstancePublicPorts	Otorga permiso para establecer los puertos abiertos especificados para una instancia y cierra todos los puertos para cada protocolo que no se incluya en la solicitud	Write	Instance*		
RebootInstance	Otorga permiso para reiniciar una instancia que se encuentra en estado de ejecución	Write	Instance*		
RebootRelationalDatabase	Otorga permiso para reiniciar una base de datos relacional que se encuentra en estado de ejecución	Write	RelationalDatabase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterContainerImage	Otorga permiso para registrar una imagen de contenedor en su servicio de contenedores de Amazon Lightsail	Write	ContainerService*		
ReleaseStaticIp	Otorga permiso para eliminar una IP estática	Write	StaticIp*		
ResetDistributionCache	Otorga permiso para eliminar contenido actualmente almacenado en caché de su distribución de la red de entrega de contenido (CDN) de Amazon Lightsail	Write	Distribution*		
SendContactMethodVerification	Otorga permiso para enviar una solicitud de verificación a un método de contacto por email a fin de asegurarse de que es propiedad del solicitante	Write			
SetIpAddressType	Otorga permiso para establecer el tipo de dirección IP de un recurso de Amazon Lightsail	Write	Distribution		
			Instance		
			LoadBalancer		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetResourceAccessForBucket	Otorga permiso para establecer los recursos de Amazon Lightsail que pueden acceder al bucket especificado de Amazon Lightsail	Escritura	Bucket* Instance*		
SetupInstanceHttps	Otorga permiso para crear un SSL/TLS certificado e instalarlo en una instancia específica	Escritura	Instance*		lightsail:GetInstanceAccessDetails
StartGUISession	Concede permiso para iniciar una sesión de interfaz gráfica de usuario (GUI) utilizada para acceder al sistema operativo o la aplicación de una instancia	Escritura	Instance*		
StartInstance	Otorga permiso para iniciar una instancia que se encuentra en estado detenido	Write	Instance*		
StartRelationalDatabase	Otorga permiso para iniciar una base de datos relacional que se encuentra en estado detenido	Escritura	RelationalDatabase*		
StopGUISession	Concede permiso para finalizar una sesión de interfaz gráfica de usuario (GUI) utilizada para acceder al sistema operativo o la aplicación de una instancia	Escritura	Instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopInstance	Otorga permiso para detener una instancia que se encuentra en estado de ejecución	Write	Instance*		
StopRelationalDatabase	Otorga permiso para detener una base de datos relacional que se encuentra en estado de ejecución	Write	RelationalDatabase*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestAlarm	Otorga permiso para probar una alarma al mostrar un banner en la consola de Amazon Lightsail o, si se configura un desencadenador de notificación para la alarma especificada, mediante el envío de una notificación al protocolo de notificación	Write	Alarm*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UnpeerVpc	Otorga permiso para tratar de quitar la interconexión de la Virtual Private Cloud (VPC) de Amazon Lightsail con la VPC predeterminada	Write			
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:TagKeys	
UpdateBucket	Otorga permiso para actualizar un bucket existente de Amazon Lightsail	Write	Bucket*		
UpdateBucketBundle	Otorga permiso para actualizar un paquete o plan de almacenamiento de un bucket existente de Amazon Lightsail	Write	Bucket*		
UpdateContainerService	Otorga permiso para actualizar la configuración de su servicio de contenedores de Amazon Lightsail, como su potencia, escala y nombres de dominio público	Write	ContainerService*		
UpdateDistribution	Otorga permiso para actualizar una distribución existente de la red de entrega de contenido (CDN) de Amazon Lightsail o su configuración	Write	Distribution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDistributionBundle	Otorga permiso para actualizar el paquete de su distribución de la red de entrega de contenido (CDN) de Amazon Lightsail	Write	Distribution*		
UpdateDomainEntry	Otorga permiso para actualizar un conjunto de registros de dominio después de crearlo	Escritura	Domain*		
UpdateInstanceMetadataOptions	Otorga permiso para actualizar las opciones de metadatos de una instancia	Escritura	Instance*		
UpdateLoadBalancerAttribute	Otorga permiso para actualizar un atributo del balanceador de carga, como la ruta de comprobación de estado y la rapidez de sesiones	Write	LoadBalancer*		
UpdateRelationalDatabase	Otorga permiso para actualizar una base de datos relacional	Write	RelationalDatabase*		
UpdateRelationalDatabaseParameters	Otorga permiso para actualizar los parámetros de una base de datos relacional	Write	RelationalDatabase*		

Tipos de recurso definidos por Amazon Lightsail

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Domain	`arn:${Partition}:lightsail:${Region}:${Account}:Domain/${Id}`	aws:ResourceTag/${TagKey}
Instance	`arn:${Partition}:lightsail:${Region}:${Account}:Instance/${Id}`	aws:ResourceTag/${TagKey}
InstanceSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:InstanceSnapshot/${Id}`	aws:ResourceTag/${TagKey}
KeyPair	`arn:${Partition}:lightsail:${Region}:${Account}:KeyPair/${Id}`	aws:ResourceTag/${TagKey}
StaticIp	`arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}`	aws:ResourceTag/${TagKey}
Disk	`arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}`	aws:ResourceTag/${TagKey}
DiskSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}`	aws:ResourceTag/${TagKey}
LoadBalancer	`arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}`	aws:ResourceTag/${TagKey}
LoadBalancerTlsCertificate	`arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}`	
ExportSnapshotRecord	`arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}`	

Tipos de recurso	ARN	Claves de condición
CloudFormationStackRecord	arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}	
RelationalDatabase	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}	aws:ResourceTag/${TagKey}
RelationalDatabaseSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}	aws:ResourceTag/${TagKey}
Alarm	arn:${Partition}:lightsail:${Region}:${Account}:Alarm/${Id}	
Certificate	arn:${Partition}:lightsail:${Region}:${Account}:Certificate/${Id}	aws:ResourceTag/${TagKey}
ContactMethod	arn:${Partition}:lightsail:${Region}:${Account}:ContactMethod/${Id}	
ContainerService	arn:${Partition}:lightsail:${Region}:${Account}:ContainerService/${Id}	aws:ResourceTag/${TagKey}
Distribution	arn:${Partition}:lightsail:${Region}:${Account}:Distribution/${Id}	aws:ResourceTag/${TagKey}
Bucket	arn:${Partition}:lightsail:${Region}:${Account}:Bucket/${Id}	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Lightsail

Amazon Lightsail define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Location

Amazon Location (prefijo de servicio: `geo`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Location
- Tipos de recurso definidos por Amazon Location
- Claves de condición de Amazon Location

Acciones definidas por Amazon Location

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateTrackerConsumer	Otorga permiso para crear una asociación entre una colección de geocercas y un recurso de rastreador	Write	tracker*		
BatchDeleteDevicePositionHistory	Otorga permiso para eliminar un lote de historiales de posición de dispositivo de un recurso de rastreador	Write	tracker*		
				geo:DeviceIds	
BatchDeleteGeofence	Otorga permiso para eliminar un lote de geocercas de una colección de geocercas	Write	geofence-collection*		
				geo:GeofenceIds	
BatchEvaluateGeofences	Otorga permiso para evaluar las posiciones del dispositivo frente a la posición de las geocercas en una colección de geocercas determinada	Write	geofence-collection*		
BatchGetDevicePosition	Otorga permiso para enviar una solicitud por lotes para recuperar las posiciones del dispositivo	Read	tracker*		
				geo:DeviceIds	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchPutGeofence	Otorga permiso para enviar una solicitud por lotes para agregar geocercas a una colección de geocercas determinada	Write	geofence-collection*		
				geo:GeofenceIds	
BatchUpdateDevicePosition	Otorga permiso para cargar una actualización de posición de uno o más dispositivos en un recurso de rastreador	Write	tracker*		
				geo:DeviceIds	
CalculateRoute	Otorga permiso para calcular rutas mediante un recurso determinado de la calculadora de rutas	Lectura	route-calculator*		
CalculateRouteMatrix	Otorga permiso para calcular una matriz de ruta con un recurso calculador de rutas determinado	Lectura	route-calculator*		
CreateGeofenceCollection	Otorga permiso para crear una colección de geocercas	Escritura	geofence-collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateKey	Concede permiso para crear un recurso de clave de API	Escritura	api-key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMap	Otorga permiso para crear un recurso de mapa	Write	map*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlaceIndex	Otorga permiso para crear un recurso de índice de ubicación	Write	place-index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouteCalculator	Otorga permiso para crear un recurso de la calculadora de rutas	Write	route-calculator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTracker	Otorga permiso para crear un recurso de rastreador	Write	tracker*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGeofenceCollection	Otorga permiso para eliminar una recopilación de geocercas	Escritura	geofence-collection*		
DeleteKey	Concede permiso para eliminar un recurso de clave de API	Escritura	api-key*		
DeleteMap	Otorga permiso para eliminar un recurso de mapa	Write	map*		
DeletePlaceIndex	Otorga permiso para eliminar un recurso de índice de ubicación	Write	place-index*		
DeleteRouteCalculator	Otorga permiso para eliminar un recurso de la calculadora de rutas	Write	route-calculator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTracker	Otorga permiso para eliminar un recurso de rastreador	Write	tracker*		
DescribeGeofenceCollection	Otorga permiso para recuperar los detalles de una recopilación de geocercas	Lectura	geofence-collection*		
DescribeKey	Concede permiso para recuperar los detalles y el secreto de un recurso de clave de API	Lectura	api-key*		
DescribeMap	Otorga permiso para recuperar los detalles de un recurso de mapa	Read	map*		
DescribePlaceIndex	Otorga permiso para recuperar los detalles de un recurso de índice de ubicación	Read	place-index*		
DescribeRouteCalculator	Otorga permiso para recuperar los detalles de un recurso de la calculadora de rutas	Read	route-calculator*		
DescribeTracker	Otorga permiso para recuperar los detalles de un recurso de rastreador	Read	tracker*		
DisassociateTrackerConsumer	Otorga permiso para eliminar la asociación entre un recurso de rastreador y una colección de geocercas	Escritura	tracker*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ForecastGeofenceEvents	Concede permiso para pronosticar eventos para geovallas almacenadas en una determinada colección de geovallas	Lectura	geofence-collection*		
GetDevicePosition	Otorga permiso para recuperar la última posición del dispositivo	Lectura	tracker*		
				geo:DeviceIds	
GetDevicePositionHistory	Otorga permiso para recuperar el historial de posiciones del dispositivo	Lectura	tracker*		
				geo:DeviceIds	
GetGeofence	Otorga permiso para recuperar los detalles de las geocercas de una colección de geocercas	Lectura	geofence-collection*		
				geo:GeofenceIds	
GetMapGlyphs	Otorga permiso para recuperar el archivo glyph de un recurso de mapa	Read	map*		
GetMapSprites	Otorga permiso para recuperar el archivo sprite de un recurso de mapa	Read	map*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMapStyleDescriptor	Otorga permiso para recuperar el descriptor de estilo de mapa de un recurso de mapa	Read	map*		
GetMapTile	Otorga permiso para recuperar el mosaico del mapa del recurso de mapa	Lectura	map*		
GetPlace	Otorga permiso para buscar un lugar por su ID único	Lectura	place-index*		
ListDevicePositions	Otorga permiso para recuperar una lista de dispositivos y sus posiciones más recientes del recurso rastreador determinado	Lectura	tracker*		
ListGeofenceCollections	Otorga permiso para enumerar las colecciones de geocercas	List	geofence-collection*		
ListGeofences	Otorga permiso para enumerar las geocercas almacenadas en una colección de geocercas determinada	Lectura	geofence-collection*		
ListKeys	Concede permiso para enumerar los recursos de clave de API	Enumeración	api-key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMaps	Otorga permiso para enumerar los recursos de mapa	List	map*		
ListPlaceIndexes	Otorga permiso para devolver una lista de los recursos de índice de ubicación	List	place-index*		
ListRouteCalculators	Otorga permiso para devolver una lista de recursos de la calculadora de rutas	List	route-calculator*		
ListTagsForResource	Concede permiso para enumerar las etiquetas (metadatos) que ha asignado al recurso.	Read	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
ListTrackerConsumers	Otorga permiso para recuperar una lista de las colecciones de geocercas actualmente asociadas al recurso de rastreador especificado	Read	tracker*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTrackers	Otorga permiso para devolver una lista de los recursos de rastreador	List	tracker*		
PutGeofence	Otorga permiso para agregar una nueva geocerca a una colección de geocercas determinada o para actualizar una geocerca existente en dicha colección	Write	geofence-collection*		
				geo:GeofenceIds	
SearchPlaceIndexForPosition	Otorga permiso para geocodificar de manera inversa una coordenada determinada	Lectura	place-index*		
SearchPlaceIndexForSuggestions	Otorga permiso para generar sugerencias para direcciones y puntos de interés basados en texto de formato libre parcial o mal escrito	Lectura	place-index*		
SearchPlaceIndexForText	Otorga permiso para geocodificar texto de formato libre, como una dirección, un nombre, una ciudad o una región	Read	place-index*		
TagResource	Otorga permiso para agregar o modificar las etiquetas del recurso especificado. Las etiquetas son metadatos que se pueden utilizar para administrar un recurso.	Etiquetado	api-key		
			geofence-collection		
			map		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			place-index		
			route-calculator		
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar las etiquetas (metadatos) dadas del recurso.	Etiquetado	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGeofenceCollection	Otorga permiso para actualizar una colección de geocercas	Escritura	geofence-collection*		
UpdateKey	Concede permiso para actualizar un recurso de clave de API	Escritura	api-key*		
UpdateMap	Otorga permiso para actualizar un recurso de mapa	Escritura	map*		
UpdatePlaceIndex	Otorga permiso para actualizar un recurso de índice de ubicación	Escritura	place-index*		
UpdateRouteCalculator	Otorga permiso para actualizar un recurso de la calculadora de rutas	Escritura	route-calculator*		
UpdateTracker	Otorga permiso para actualizar un recurso de rastreador	Escritura	tracker*		
VerifyDevicePosition	Concede permiso para verificar la posición de un dispositivo	Lectura	tracker*		
				geo:DeviceIds	

Tipos de recurso definidos por Amazon Location

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
api-key	`arn:${Partition}:geo:${Region}:${Account}:api-key/${KeyName}`	aws:ResourceTag/${TagKey}
geofence-collection	`arn:${Partition}:geo:${Region}:${Account}:geofence-collection/${GeofenceCollectionName}`	aws:ResourceTag/${TagKey} geo:GeofenceIds
map	`arn:${Partition}:geo:${Region}:${Account}:map/${MapName}`	aws:ResourceTag/${TagKey}
place-index	`arn:${Partition}:geo:${Region}:${Account}:place-index/${IndexName}`	aws:ResourceTag/${TagKey}
route-calculator	`arn:${Partition}:geo:${Region}:${Account}:route-calculator/${CalculatorName}`	aws:ResourceTag/${TagKey}
tracker	`arn:${Partition}:geo:${Region}:${Account}:tracker/${TrackerName}`	aws:ResourceTag/${TagKey} geo:DeviceIds

Claves de condición de Amazon Location

Amazon Location define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString
geo:DeviceIds	Filtra el acceso por la presencia de ID de dispositivos en la solicitud	ArrayOfString
geo:GeofenceIds	Filtra el acceso por la presencia de ID de geocercas en la solicitud	ArrayOfString

Claves de estado, recursos y acciones de Amazon Location Service Maps

Amazon Location Service Maps (prefijo de servicio:`geo-maps`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Location Service Maps
- Tipos de recursos definidos por Amazon Location Service Maps
- Claves de estado de Amazon Location Service Maps

Acciones definidas por Amazon Location Service Maps

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetStaticMap	Otorga permiso para recuperar el mapa estático	Lectura	provider*		
GetTile	Otorga permiso para recuperar el mosaico del mapa	Lectura	provider*		

Tipos de recursos definidos por Amazon Location Service Maps

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
provider	`arn:${Partition}:geo-maps:${Region}::provider/default`	

Claves de estado de Amazon Location Service Maps

Geo Maps no tiene claves de contexto específicas de un servicio que puedan usarse como `Condition` elemento de las declaraciones de políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de Amazon Location Service Places

Amazon Location Service Places (prefijo de servicio:`geo-places`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Location Service Places
- Tipos de recursos definidos por Amazon Location Service Places
- Claves de estado de Amazon Location Service Places

Acciones definidas por Amazon Location Service Places

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Autocomplete	Otorga permiso para completar automáticamente la entrada de texto con posibles lugares y direcciones a medida que el usuario escribe	Lectura	provider*		
Geocode	Otorga permiso para geocodificar una dirección o un lugar	Lectura	provider*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	textual en coordenadas geográficas				
GetPlace	Otorga permiso para consultar un lugar por su identificador de lugar único	Lectura	provider*		
ReverseGeocode	Otorga permiso para convertir las coordenadas geográficas en una dirección o un lugar legibles para los humanos	Lectura	provider*		
SearchNearby	Otorga permiso para recuperar lugares cercanos a una posición que coincidan con un conjunto de restricciones definidas por el usuario, como la categoría o el tipo de comida que ofrece el lugar	Lectura	provider*		
SearchText	Otorga permiso para buscar lugares mediante una sola entrada de texto de formato libre	Lectura	provider*		
Suggest	Otorga permiso para sugerir posibles lugares en función de las entradas del usuario	Lectura	provider*		

Tipos de recursos definidos por Amazon Location Service Places

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
provider	`arn:${Partition}:geo-places:${Region}::provider/default`	

Claves de estado de Amazon Location Service Places

Geo Places no tiene claves de contexto específicas de un servicio que puedan usarse como `Condition` elemento de las declaraciones de políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS global.

Claves de estado, recursos y acciones de Amazon Location Service Routes

Amazon Location Service Routes (prefijo de servicio:`geo-routes`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Location Service Routes
- Tipos de recursos definidos por las rutas de Amazon Location Service
- Claves de estado de las rutas de Amazon Location Service

Acciones definidas por Amazon Location Service Routes

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CalculateIsolines	Otorga permiso para determinar los destinos o las áreas de servicio a las que se puede llegar en un tiempo específico	Lectura	provider*		
CalculateRouteMatrix	Otorga permiso para calcular la matriz de rutas, que proporciona el tiempo de viaje y las distancias entre conjuntos de orígenes y destinos	Lectura	provider*		
CalculateRoutes	Otorga permiso para calcular rutas entre dos o más ubicaciones	Lectura	provider*		
OptimizeWaypoints	Otorga permiso para calcular la secuencia más eficiente para visitar varios puntos de referencia o ubicaciones a lo largo de una ruta	Lectura	provider*		
SnapToRoads	Concede permiso para mejorar la precisión del posicionamiento geográfico al alinear las coordenadas del GPS con los segmentos de carretera más cercanos de un mapa digital	Lectura	provider*		

Tipos de recursos definidos por las rutas de Amazon Location Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
provider	`arn:${Partition}:geo-routes:${Region}::provider/default`	

Claves de estado de las rutas de Amazon Location Service

Geo Routes no tiene claves de contexto específicas de un servicio que puedan usarse como `Condition` elemento de las declaraciones de políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Lookout for Equipment

Amazon Lookout for Equipment (prefijo de servicio: `lookoutequipment`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para usarlos en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Lookout for Equipment
- Tipos de recursos definidos por Amazon Lookout for Equipment
- Claves de condición para Amazon Lookout for Equipment

Acciones definidas por Amazon Lookout for Equipment

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataset	Concede permiso para crear un conjunto de datos	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceScheduler	Concede permiso para crear un programador de inferencias para un modelo entrenado	Escritura	inference-scheduler*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabel	Concede permiso para crear una etiqueta	Escritura	label-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLabelGroup	Concede permiso para crear un grupo de etiquetas	Escritura	label-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Concede permiso para crear un modelo entrenado con un conjunto de datos	Escritura	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetrainingScheduler	Concede permiso para crear un programador de reentrenamiento para un modelo entrenado	Escritura	model*		
DeleteDataset	Concede permiso para eliminar un conjunto de datos	Write	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteInferenceScheduler	Concede permiso para eliminar un programador de inferencias	Escritura	inference-scheduler*		
DeleteLabel	Concede permiso para eliminar una etiqueta	Escritura	label-group*		
DeleteLabelGroup	Concede permiso para eliminar un grupo de etiquetas	Escritura	label-group*		
DeleteModel	Concede permiso para eliminar un modelo	Escritura	model*		
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos.	Escritura	dataset		
			model		
			model-version		
DeleteRetrainingScheduler	Concede permiso para eliminar un programador de reentrenamiento de un modelo entrenado	Escritura	model*		
DescribeDataIngestionJob	Concede permiso para describir un trabajo de incorporación de datos	Read			
DescribeDataset	Concede permiso para describir un conjunto de datos	Read	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInferenceScheduler	Concede permiso para describir un programador de inferencias	Lectura	inference-scheduler*		
DescribeLabelGroup	Concede permiso para describir un grupo de etiquetas	Lectura	label-group*		
DescribeModel	Concede permiso para describir un modelo	Lectura	model*		
DescribeModelVersion	Concede permiso para describir una versión de modelo	Lectura	model-version*		
DescribeResourcePolicy	Concede permiso para describir una política de recurso	Lectura	dataset		
			model		
			model-version		
DescribeRetrainingScheduler	Concede permiso para describir un programador de reentrenamiento de un modelo entrenado	Lectura	model*		
Describelabel	Concede permiso para describir una etiqueta	Lectura	label-group*		
ImportDataset	Concede permiso para importar un conjunto de datos	Escritura	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportModelVersion	Concede permiso para importar una versión de modelo	Escritura	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys lookoutequipment:IsImportingData	
ListDataIngestionJobs	Concede permiso para enumerar los trabajos de incorporación de datos en su cuenta o para un conjunto de datos determinado	List	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDatasets	Concede permiso para enumerar los conjuntos de datos de la cuenta	Enumeración			
ListInferenceEvents	Concede permiso para enumerar los eventos de inferencia de un programador de inferencias	Lectura	inference-scheduler*		
ListInferenceExecutions	Concede permiso para enumerar las ejecuciones de inferencia para un programador de inferencias	Read	inference-scheduler*		
ListInferenceSchedulers	Concede permiso para enumerar los programadores de inferencias en la cuenta	Enumeración			
ListLabelGroups	Concede permiso para enumerar los grupos de etiquetas en su cuenta	Enumeración	label-group*		
ListLabels	Concede permiso para enumerar las etiquetas en su cuenta	Enumeración	label-group*		
ListModelVersions	Concede permiso para enumerar las versiones de modelo en la cuenta	Enumeración	model*		
ListModels	Concede permiso para enumerar los modelos en la cuenta.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRetrainingSchedulers	Concede permiso para enumerar los programadores de reentrenamiento en la cuenta	Enumeración			
ListSensorStatistics	Concede permiso para enumerar las estadísticas de sensores para un conjunto de datos determinado o para un trabajo de incorporación	Enumeración	dataset*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
PutResourcePolicy	Concede permiso para colocar una política de recursos	Escritura	dataset		
			model		
			model-version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDataIngestionJob	Concede permiso para iniciar un trabajo de incorporación de datos para un conjunto de datos	Write	dataset*		
StartInferenceScheduler	Concede permiso para iniciar un programador de inferencias	Escritura	inference-scheduler*		
StartRetrainingScheduler	Concede permiso para iniciar un programador de reentrenamiento de un modelo entrenado	Escritura	model*		
StopInferenceScheduler	Concede permiso para detener un programador de inferencias	Escritura	inference-scheduler*		
StopRetrainingScheduler	Concede permiso para detener un programador de reentrenamiento de un modelo entrenado	Escritura	model*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	dataset inference-scheduler		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			label-group		
			model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateActiveModelVersion	Concede permiso para establecer la versión de modelo activo para un modelo de machine learning determinado	Escritura	model* model-version*		
UpdateInferenceScheduler	Concede permiso para actualizar un programador de inferencias	Escritura	inference-scheduler*		
UpdateLabelGroup	Concede permiso para actualizar un grupo de etiquetas	Escritura	label-group*		
UpdateModel	Concede permiso para actualizar un modelo	Escritura	model*		
UpdateRetrainingScheduler	Concede permiso para actualizar un programador de reentrenamiento de un modelo entrenado	Escritura	model*		

Tipos de recursos definidos por Amazon Lookout for Equipment

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
dataset	`arn:${Partition}:lookoutequipment:${Region}:${Account}:dataset/${DatasetName}/${DatasetId}`	aws:ResourceTag/${TagKey}
model	`arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}`	aws:ResourceTag/${TagKey}
model-version	`arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}/model-version/${ModelVersionNumber}`	aws:ResourceTag/${TagKey}
inference-scheduler	`arn:${Partition}:lookoutequipment:${Region}:${Account}:inference-scheduler/${InferenceSchedulerName}/${InferenceSchedulerId}`	aws:ResourceTag/${TagKey}
label-group	`arn:${Partition}:lookoutequipment:${Region}:${Account}:label-group/${LabelGroupName}/${LabelGroupId}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Lookout for Equipment

Amazon Lookout for Equipment define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
lookoutequipment:IsImportingData	Filtra el acceso según la estrategia de importación de datos subyacentes	Bool

Acciones, recursos y claves de condición para Amazon Lookout for Metrics

Amazon Lookout for Metrics (prefijo de servicio: `lookoutmetrics`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Lookout for Metrics
- Tipos de recursos definidos por Amazon Lookout for Metrics
- Claves de condición de Amazon Lookout for Metrics

Acciones definidas por Amazon Lookout for Metrics

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateAnomalyDetector	Otorga permiso para activar un detector de anomalías	Write	AnomalyDetector*		
BackTestAnomalyDetector	Otorga permiso para ejecutar una prueba inversa con un detector de anomalías	Write	AnomalyDetector*		
CreateAlert	Otorga permiso para crear una alerta para un detector de anomalías	Write	Alert*		
			AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalyDetector	Otorga permiso para crear un detector de anomalías	Write	AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMetricSet	Concede permiso para crear un conjunto de datos	Escritura	AnomalyDetector*		
			MetricSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateAnomalyDetector	Otorga permiso para desactivar un detector de anomalías	Escritura	AnomalyDetector*		
DeleteAlert	Otorga permiso para eliminar una alerta	Write	Alert*		
DeleteAnomalyDetector	Otorga permiso para eliminar un detector de anomalías	Write	AnomalyDetector*		
DescribeAlert	Otorga permiso para obtener detalles acerca de una alerta	Read	Alert*		
DescribeAnomalyDetectionExecutions	Otorga permiso para obtener información sobre un trabajo de detección de anomalías	Read	AnomalyDetector*		
DescribeAnomalyDetector	Otorga permiso para obtener detalles sobre un detector de anomalías	Read	AnomalyDetector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMetricSet	Otorga permiso para obtener detalles acerca de un conjunto de datos	Lectura	MetricSet*		
DetectMetricSetConfig	Otorga permiso para detectar la configuración del conjunto de métricas desde el origen de datos	Escritura	AnomalyDetector*		
GetAnomalyGroup	Otorga permiso para obtener detalles sobre un grupo de métricas afectadas	Read	AnomalyDetector*		
GetDataQualityMetrics	Otorga permiso para obtener métricas de calidad de datos para un detector de anomalías	Read	AnomalyDetector*		
GetFeedback	Otorga permiso para obtener comentarios sobre las métricas afectadas para un grupo de anomalías	Read	AnomalyDetector*		
GetSampleData	Otorga permiso para obtener una selección de registros de muestra de un origen de datos de Amazon S3	Read			
ListAlerts	Otorga permiso para obtener una lista de alertas para un detector	List	AnomalyDetector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAnomalyDetectors	Otorga permiso para obtener una lista de detectores de anomalías	Enumeración			
ListAnomalyGroupRelatedMetrics	Otorga permiso para obtener una lista de mediciones relacionadas en un grupo de anomalías	Enumeración	AnomalyDetector*		
ListAnomalyGroupSummaries	Otorga permiso para obtener una lista de grupos de anomalías	List	AnomalyDetector*		
ListAnomalyGroupTimeSeries	Otorga permiso para obtener una lista de métricas afectadas para una medida de un grupo de anomalías	List	AnomalyDetector*		
ListMetricSets	Otorga permiso para obtener una lista de conjuntos de datos	List	AnomalyDetector		
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas para un detector, conjunto de datos o alerta	Read	Alert		
			AnomalyDetector		
			MetricSet		
PutFeedback	Otorga permiso para agregar comentarios para una métrica afectada en un grupo de anomalías	Write	AnomalyDetector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar etiquetas a un detector, conjunto de datos o alerta	Etiquetado	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para quitar etiquetas de un detector, conjunto de datos o alerta	Etiquetado	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys	
UpdateAlert	Otorga permiso para actualizar una alerta para un detector de anomalías	Escritura	Alert*		
UpdateAnomalyDetector	Otorga permiso para actualizar un detector de anomalías	Write	AnomalyDetector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMetricSet	Concede permiso para actualizar un conjunto de datos	Write	MetricSet *		

Tipos de recursos definidos por Amazon Lookout for Metrics

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AnomalyDetector	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:AnomalyDetector:${AnomalyDetectorName}`	aws:ResourceTag/${TagKey}
MetricSet	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:MetricSet/${AnomalyDetectorName}/${MetricSetName}`	aws:ResourceTag/${TagKey}
Alert	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:Alert:${AlertName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Lookout for Metrics

Amazon Lookout for Metrics define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Lookout for Vision

Amazon Lookout for Vision (prefijo de servicio: `lookoutvision`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Lookout for Vision
- Tipos de recursos definidos por Amazon Lookout for Vision
- Claves de condición de Amazon Lookout for Vision

Acciones definidas por Amazon Lookout for Vision

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataset	Concede permiso para crear un manifiesto de conjunto de datos	Write			
CreateModel	Concede permiso para crear un nuevo modelo de detección de anomalías	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Concede permiso para crear un nuevo proyecto	Write	project*		
DeleteDataset	Concede permiso para eliminar un conjunto de datos	Write			
DeleteModel	Concede permiso para eliminar un modelo y todos los recursos asociados	Write	model*		
DeleteProject	Concede permiso para eliminar permanentemente un proyecto	Write	project*		
DescribeDataset	Concede permiso para mostrar información detallada sobre el manifiesto de conjunto de datos	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeModel	Concede permiso para mostrar información detallada acerca de un modelo	Lectura	model*		
DescribeModelPackagingJob	Concede permiso para mostrar información detallada acerca de un trabajo de empaquetado de modelo	Lectura			
DescribeProject	Concede permiso para mostrar información detallada sobre un proyecto	Read	project*		
DescribeTrialDetection [solo permiso]	Concede permiso para proporcionar la información del estado de un trabajo de detección de anomalías en ejecución	Read			
DetectAnomalies	Concede permiso para invocar la detección de anomalías	Write	model*		
ListDatasetEntries	Concede permiso para enumerar el contenido del manifiesto de conjunto de datos	Lectura			
ListModelPackagingJobs	Concede permiso para enumerar todos los trabajos de empaquetado de modelos asociados a un proyecto	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListModels	Concede permiso para enumerar todos los modelos asociados a un proyecto	List			
ListProjects	Concede permiso para enumerar todos los proyectos	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	model		
ListTrialDetections [solo permiso]	Concede permiso para enumerar todos los trabajos de detección de anomalías	List			
StartModel	Concede permiso para iniciar el modelo de detección de anomalías	Escritura	model*		
StartModelPackagingJob	Concede permiso para iniciar un trabajo de empaquetado de modelos	Escritura	model*		
StartTrialDetection [solo permiso]	Concede permiso para iniciar la detección masiva de anomalías para un conjunto de imágenes almacenadas en un bucket de S3	Write			
StopModel	Concede permiso para detener el modelo de detección de anomalías	Escritura	model*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	model		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar de un recurso la etiqueta con la clave dada	Etiquetado	model		
				aws:TagKeys	
UpdateDatasetEntries	Concede permiso para actualizar un manifiesto de conjunto de datos de entrenamiento o prueba	Write			

Tipos de recursos definidos por Amazon Lookout for Vision

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
model	arn:${Partition}:lookoutvision:${Region}:${Account}:model/${ProjectName}/${ModelVersion}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:lookoutvision:${Region}:${Account}:project/${ProjectName}	

Claves de condición de Amazon Lookout for Vision

Amazon Lookout for Vision define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Machine Learning

Amazon Machine Learning (prefijo de servicio: `machinelearning`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Machine Learning
- Tipos de recurso definidos por Amazon Machine Learning
- Claves de condición de Amazon Machine Learning

Acciones definidas por Amazon Machine Learning

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTags	Agrega una o varias etiquetas a un objeto, hasta un límite de 10. Cada etiqueta consta de una clave y un valor opcional	Etiquetado	batchprediction		
			datasource		
			evaluation		
			mlmodel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBatchPrediction	Genera predicciones para un grupo de observaciones.	Escritura	batchprediction*		
			datasource*		
			mlmodel*		
CreateDataSourceFromRDS	Crea un DataSource objeto a partir de un Amazon RDS	Escritura	datasource*		
CreateDataSourceFromRedshift	Crea un DataSource a partir de una base de datos alojada en un clúster de Amazon Redshift	Escritura	datasource*		
CreateDataSourceFromS3	Crea un DataSource objeto a partir de S3	Escritura	datasource*		
CreateEvaluation	Crea una nueva evaluación de un MLModel	Escritura	datasource*		
			evaluation*		
			mlmodel*		
CreateMLModel	Crea una nueva MLModel	Escritura	datasource*		
			mlmodel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRealtimeEndpoint	Crea un punto final en tiempo real para el MLModel	Escritura	mlmodel*		
DeleteBatchPrediction	Asigna el estado ELIMINADO a BatchPrediction, lo que lo deja inutilizable	Escritura	batchprediction*		
DeleteDataSource	Asigna el estado ELIMINADO a DataSource, por lo que queda inutilizable	Escritura	datasource*		
DeleteEvaluation	Asigna el estado DELETED a una evaluación, lo que la deja inutilizable.	Escritura	evaluation*		
DeleteMLModel	Asigna el estado ELIMINADO a un, lo que lo deja MLModel inutilizable	Escritura	mlmodel*		
DeleteRealtimeEndpoint	Elimina un punto final en tiempo real de un MLModel	Escritura	mlmodel*		
DeleteTags	Elimina las etiquetas especificadas asociadas a un objeto ML. Después de que esta operación se haya completado, no se pueden recuperar las etiquetas eliminadas.	Etiquetado	batchprediction		
			datasource		
			evaluation		
			mlmodel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBatchPredictions	Devuelve una lista de BatchPrediction operaciones que coinciden con los criterios de búsqueda de la solicitud	Enumeración			
DescribeDataSources	Devuelve una lista de las DataSource que coinciden con los criterios de búsqueda de la solicitud	Enumeración			
DescribeEvaluations	Devuelve una lista de los DescribeEvaluations que coinciden con los criterios de búsqueda de la solicitud	Enumeración			
DescribeMLModels	Devuelve una lista de los MLModel que coinciden con los criterios de búsqueda de la solicitud	Enumeración			
DescribeTags	Describe una o varias de las etiquetas para su objeto de Amazon ML.	Enumeración	batchprediction		
			datasource		
			evaluation		
			mlmodel		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBatchPrediction	Devuelve un BatchPrediction que incluye información detallada sobre los metadatos, el estado y el archivo de datos	Lectura	batchprediction*		
GetDataSource	Devuelve un DataSource que incluye información sobre los metadatos y el archivo de datos, así como el estado actual del DataSource	Lectura	datasource*		
GetEvaluation	Devuelve una evaluación que incluye metadatos, así como el estado actual de la evaluación.	Lectura	datasource*		
GetMLModel	Devuelve un valor MLModel que incluye información detallada sobre los metadatos y la fuente de datos, así como el estado actual del MLModel	Lectura	mlmodel*		
Predict	Genera una predicción para la observación utilizando el modelo de ML especificado.	Escritura	mlmodel*		
UpdateBatchPrediction	Actualiza el BatchPredictionName de un BatchPrediction	Escritura	batchprediction*		
UpdateDataSource	Actualiza el DataSourceName de un DataSource	Escritura	datasource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEvaluation	Actualiza la EvaluationName de una evaluación	Escritura	evaluation*		
UpdateMLModel	Actualiza el MLModel nombre y el ScoreThreshold de un MLModel	Escritura	mlmodel*		

Tipos de recurso definidos por Amazon Machine Learning

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	
evaluation	`arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}`	

Tipos de recurso	ARN	Claves de condición
mlmodel	`arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}`	

Claves de condición de Amazon Machine Learning

Machine Learning no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Macie

Amazon Macie (prefijo de servicio: `macie2`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Macie
- Tipos de recursos definidos por Amazon Macie
- Claves de condición de Amazon Macie

Acciones definidas por Amazon Macie

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Las GetMasterAccount acciones DisassociateFromMasterAccount y han quedado en desuso. En su lugar, le recomendamos que especifique las GetAdministratorAccount acciones DisassociateFromAdministratorAccount y las acciones respectivamente.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptInvitation	Otorga permiso para aceptar una invitación de suscripción a Amazon Macie	Write			
BatchGetCustomDataIdentifiers	Otorga permiso para recuperar información sobre uno o más identificadores de datos personalizados	Lectura	CustomDataIdentifier*		
BatchUpdateAutomatedDiscoveryAccounts	Concede permiso a un administrador de Amazon Macie para cambiar el estado del descubrimiento automatizado de datos confidenciales para una o varias cuentas de su organización	Escritura			
CreateAllowList	Otorga permiso para crear y definir la configuración de una lista de permitidos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateClassificationJob	Otorga permiso para crear y definir la configuración de un	Write	ClassificationJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	trabajo de descubrimiento de información confidencial.			aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDataIdentifier	Otorga permiso para crear y definir la configuración de un identificador de datos personalizado	Write	CustomDataIdentifier*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsFilter	Concede permiso para crear y definir la configuración de un filtro de resultados	Write	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvitations	Otorga permiso para enviar una invitación de suscripción a Amazon Macie	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMember	Otorga permiso para asociar una cuenta con una cuenta de administrador de Amazon Macie.	Write	Member*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSampleFindings	Otorga permiso para crear hallazgos de muestra	Write			
DeclineInvitations	Otorga permiso para rechazar invitaciones de suscripción a Amazon Macie	Escritura			
DeleteAllowList	Otorga permiso para eliminar una lista de permitidos	Escritura	AllowList*		
DeleteCustomDataIdentifier	Otorga permiso para eliminar un identificador de datos personalizado	Write	CustomDataIdentifier*		
DeleteFindingsFilter	Otorga permiso para eliminar un filtro de hallazgos	Write	FindingsFilter*		
DeleteInvitations	Otorga permiso para eliminar invitaciones de suscripción a Amazon Macie	Write			
DeleteMember	Otorga permiso para eliminar la asociación entre una cuenta y una cuenta de administrador de Amazon Macie.	Write	Member*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBuckets	Otorga permiso para recuperar datos estadísticos e información de otro tipo sobre los buckets de S3 que Amazon Macie monitorea y analiza.	Read			
DescribeClassificationJob	Otorga permiso para recuperar información sobre el estado y la configuración de un trabajo de descubrimiento de información confidencial.	Lectura	ClassificationJob*		
DescribeOrganizationConfiguration	Otorga permiso para recuperar información sobre los ajustes de configuración de Amazon Macie de una organización AWS	Lectura			
DisableMacie	Otorga permiso para desactivar una cuenta de Amazon Macie, que también elimina los recursos de Macie de la cuenta	Escritura			
DisableOrganizationAdminAccount	Otorga permiso para deshabilitar una cuenta como cuenta de administrador delegado de Amazon Macie para una organización AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateFromAdministratorAccount	Otorga permiso a una cuenta de miembro de Amazon Macie para desasociarse de su cuenta de administrador de Macie	Escritura			
DisassociateFromMasterAccount	Otorga permiso a una cuenta de miembro de Amazon Macie para desasociarse de su cuenta de administrador de Macie	Escritura			
DisassociateMember	Otorga permiso a una cuenta de administrador de Amazon Macie para desasociarse de una cuenta de miembro de Macie	Escritura	Member*		
EnableMacie	Otorga permiso para habilitar y especificar la configuración de una nueva cuenta de Amazon Macie	Escritura			
EnableOrganizationAdminAccount	Otorga permiso para habilitar una cuenta como cuenta de administrador delegado de Amazon Macie para una organización AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAdministratorAccount	Otorga permiso para recuperar información sobre la cuenta de administrador de Amazon Macie para una cuenta	Lectura			
GetAllowList	Otorga permiso para recuperar la configuración y el estado de una lista de permitidos	Lectura	AllowList*		
GetAutomatedDiscoveryConfiguration	Concede permiso para obtener los ajustes de configuración y el estado de la detección automatizada de datos confidenciales para una cuenta de administrador, organización o cuenta independiente de Amazon Macie	Lectura			
GetBucketStatistics	Otorga permiso para recuperar datos estadísticos agregados para todos los buckets de S3 que Amazon Macie monitorea y analiza	Read			
GetClassificationExportConfiguration	Otorga permiso para recuperar la configuración para exportar los resultados del descubrimiento de información confidencial.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetClassificationScope	Otorga permiso para recuperar la configuración del ámbito de clasificación de una cuenta	Lectura			
GetCustomDataIdentifier	Otorga permiso para recuperar información sobre la configuración de un identificador de datos personalizado	Read	CustomDataIdentifier*		
GetFindingStatistics	Otorga permiso para recuperar datos estadísticos agregados sobre hallazgos	Read			
GetFindings	Otorga permiso para recuperar los detalles de uno o más hallazgos.	Read			
GetFindingsFilter	Otorga permiso para recuperar información sobre la configuración de un filtro de hallazgos	Lectura	FindingsFilter*		
GetFindingsPublicationConfiguration	Otorga permiso para recuperar los ajustes de configuración para publicar los hallazgos en AWS Security Hub	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetInvitationsCount	Otorga permiso para recuperar el recuento de invitaciones de suscripción a Amazon Macie recibidas por una cuenta	Read			
GetMacieSession	Otorga permiso para recuperar información sobre el estado y la configuración de una cuenta de Amazon Macie	Lectura			
GetMasterAccount	Otorga permiso para recuperar información sobre la cuenta de administrador de Amazon Macie para una cuenta	Lectura			
GetMember	Otorga permiso para recuperar información sobre una cuenta asociada a una cuenta de administrador de Amazon Macie.	Lectura	Member*		
GetResourceProfile	Otorga permiso para recuperar las estadísticas de descubrimiento de información confidencial y la puntuación de confidencialidad de un bucket de S3	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRevealConfiguration	Otorga permiso para recuperar los ajustes del estado y la configuración para recuperar las ocurrencias de datos confidenciales informados por los hallazgos	Lectura			
GetSensitiveDataOccurrences	Otorga permiso para recuperar las ocurrencias de datos confidenciales informados por un hallazgo	Lectura			
GetSensitiveDataOccurrencesAvailability	Otorga permiso para verificar si las ocurrencias de datos confidenciales pueden recuperarse por un hallazgo	Lectura			
GetSensitivityInspectionTemplate	Otorga permiso para recuperar la configuración de la plantilla de inspección de confidencialidad de una cuenta	Lectura			
GetUsageStatistics	Otorga permiso para recuperar cuotas y datos de uso agregados para una o varias cuentas	Read			
GetUsageTotals	Otorga permiso para recuperar datos de uso agregados de una cuenta	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAllowLists	Otorga permiso para recuperar un subconjunto de información sobre todas las listas de permitidos de una cuenta	Enumeración			
ListAutomatedDiscoveryAccounts	Concede permiso para obtener el estado de la detección automática de datos confidenciales de una cuenta	Enumeración			
ListClassificationJobs	Otorga permiso para recuperar un subconjunto de datos sobre el estado y la configuración de uno o más trabajos de descubrimiento de información confidencial.	Enumeración			
ListClassificationScopes	Otorga permiso para recuperar un subconjunto de información sobre el ámbito de clasificación de una cuenta	Enumeración			
ListCustomDataIdentifiers	Otorga permiso para recuperar información sobre todos los identificadores de datos personalizados	List			
ListFindings	Otorga permiso para recuperar un subconjunto de información sobre uno o más hallazgos	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFindingsFilters	Otorga permiso para recuperar información sobre todos los filtros de hallazgos	List			
ListInvitations	Otorga permiso para recuperar información sobre todas las invitaciones de suscripción a Amazon Macie recibidas por una cuenta	Enumeración			
ListManagedDataIdentifiers	Otorga permiso para recuperar información sobre los identificadores de datos administrados	Enumeración			
ListMembers	Otorga permiso para recuperar información sobre las cuentas de miembro de Amazon Macie asociadas a una cuenta de administrador de Macie.	Enumeración			
ListOrganizationAdminAccounts	Otorga permiso para recuperar información sobre la cuenta de administrador delegada de Amazon Macie de una organización AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourceProfileArtifacts	Concede permiso para recuperar información sobre objetos que Amazon Macie seleccionó de un bucket de S3 para el descubrimiento automatizado de datos confidenciales	Enumeración			
ListResourceProfileDetections	Otorga permiso para recuperar información sobre los tipos y la cantidad de información confidencial que Amazon Macie encontró en un bucket de S3	Enumeración			
ListSensitivityInspectionTemplates	Otorga permiso para recuperar un subconjunto de información sobre la plantilla de inspección de confidencialidad de una cuenta	Enumeración			
ListTagsForResource	Otorga permiso para recuperar las etiquetas de un recurso de Amazon Macie.	Read	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Member		
PutClassificationExportConfiguration	Otorga permiso para crear o actualizar la configuración para el almacenamiento de los resultados del descubrimiento de información confidencial.	Escritura			
PutFindingsPublicationConfiguration	Otorga permiso para actualizar los ajustes de configuración para publicar los hallazgos en AWS Security Hub	Escritura			
SearchResources	Otorga permiso para recuperar datos estadísticos y otra información sobre AWS los recursos que Amazon Macie monitorea y analiza	Lectura			
TagResource	Otorga permiso para agregar o actualizar las etiquetas de un recurso de Amazon Macie.	Etiquetado	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
TestCustomDataIdentifier	Otorga permiso para probar un identificador de datos personalizado	Write			
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de Amazon Macie.	Etiquetado	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:TagKeys	
UpdateAllowList	Otorga permiso para actualizar la configuración de una lista de permitidos	Escritura	AllowList*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAutomatedDiscoveryConfiguration	Concede permiso para cambiar el estado del descubrimiento automatizado de datos confidenciales para una cuenta de administrador, organización o cuenta independiente de Amazon Macie	Escritura			
UpdateClassificationJob	Otorga permiso para cambiar el estado de un trabajo de descubrimiento de información confidencial.	Escritura	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateClassificationScope	Otorga permiso para actualizar la configuración del ámbito de clasificación de una cuenta	Escritura			
UpdateFindingsFilter	Otorga permiso para actualizar la configuración de un filtro de hallazgos	Escritura	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMacieSession	Concede permiso a una cuenta de administrador de Amazon Macie para suspender o volver a habilitar Macie para una cuenta de miembro	Escritura			
UpdateMemberSession	Otorga permiso a una cuenta de administrador de Amazon Macie para suspender o volver a habilitar una cuenta de miembro de Macie	Escritura			
UpdateOrganizationConfiguration	Otorga permiso para actualizar los ajustes de configuración de Amazon Macie de una organización AWS	Escritura			
UpdateResourceProfile	Otorga permiso para actualizar la puntuación de confidencialidad de un bucket de S3	Escritura			
UpdateResourceProfileDetections	Otorga permiso para actualizar la configuración de la puntuación de confidencialidad de un bucket de S3	Escritura			
UpdateRevealConfiguration	Otorga permiso para actualizar los ajustes del estado y la configuración para recuperar las ocurrencias de datos confidenciales informados por los hallazgos	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSensitivityInspectionTemplate	Otorga permiso para actualizar la configuración de la plantilla de inspección de confidencialidad de una cuenta	Escritura			

Tipos de recursos definidos por Amazon Macie

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AllowList	`arn:${Partition}:macie2:${Region}:${Account}:allow-list/${ResourceId}`	aws:ResourceTag/${TagKey}
ClassificationJob	`arn:${Partition}:macie2:${Region}:${Account}:classification-job/${ResourceId}`	aws:ResourceTag/${TagKey}
CustomDataIdentifier	`arn:${Partition}:macie2:${Region}:${Account}:custom-data-identifier/${ResourceId}`	aws:ResourceTag/${TagKey}
FindingsFilter	`arn:${Partition}:macie2:${Region}:${Account}:findings-filter/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Member	`arn:${Partition}:macie2:${Region}:${Account}:member/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Macie

Amazon Macie define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para las Pruebas de aplicaciones de AWS Mainframe Modernization

AWS Las pruebas de aplicaciones de modernización de mainframe (prefijo de servicio:`apptest`) proporcionan los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las Pruebas de aplicaciones de AWS Mainframe Modernization
- Tipos de recursos definidos por las Pruebas de aplicaciones de AWS Mainframe Modernizations
- Claves de condición para las Pruebas de aplicaciones de AWS Mainframe Modernization

Acciones definidas por las Pruebas de aplicaciones de AWS Mainframe Modernization

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTestCase	Concede permiso para crear un caso de prueba	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestConfiguration	Concede permiso para crear una configuración de la prueba	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTestSuite	Concede permiso para crear un conjunto de pruebas	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTestCase	Concede permiso para eliminar un caso de prueba	Escritura	TestCase*		
DeleteTestConfiguration	Concede permiso para eliminar una configuración de la prueba	Escritura	TestConfiguration*		
DeleteTestRun	Concede permiso para eliminar una ejecución de prueba	Escritura	TestRun*		s3:DeleteObject s3:ListBucket
DeleteTestSuite	Concede permiso para eliminar un conjunto de pruebas	Escritura	TestSuite*		
GetTestCase	Concede permiso para obtener un caso de prueba	Lectura	TestCase*		
GetTestConfiguration	Concede permiso para obtener una configuración de la prueba	Lectura	TestConfiguration*		
GetTestRunStep	Concede permiso para obtener el paso de ejecución de prueba	Lectura	TestRun*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTestSuite	Concede permiso para obtener un conjunto de pruebas	Lectura	TestSuite*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
ListTestCases	Concede permiso para enumerar casos de prueba	Enumeración			
ListTestConfigurations	Concede permiso para enumerar configuraciones de la prueba	Enumeración			
ListTestRunSteps	Concede permiso para enumerar los pasos de una ejecución de prueba	Lectura	TestRun*		
ListTestRunTestCases	Concede permiso para enumerar casos de prueba de una ejecución de prueba	Lectura	TestRun*		
ListTestRuns	Concede permiso para enumerar ejecuciones de pruebas	Enumeración			
ListTestSuites	Concede permiso para enumerar conjuntos de pruebas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartTestRun	Concede permiso para iniciar una ejecución de prueba	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:CreateStack cloudformation:DeleteStack cloudformation:DescribeStacks dms:DescribeReplicationTasks dms:StartReplicationTask dms:StopReplicationTask ec2:DescribeAvailabilityZones ec2:DescribeVpcEndpointServ

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iceConfigurations ec2:DescribeVpcEndpointServices m2:CreateDataSetImportTask m2:GetApplication m2:GetApplicationVersion m2:GetBatchJobExecution m2:GetDataSetDetails m2:GetDataSetImportTask m2:StartApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					m2:StartBatchJob m2:StopApplication s3:CreateBucket s3:DeleteObject s3:GetObject s3:ListBucket s3:PutObject
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		
				aws:TagKeys	
UpdateTestCase	Concede permiso para actualizar un caso de prueba	Escritura	TestCase*		
UpdateTestConfiguration	Concede permiso para actualizar una configuración de la prueba	Escritura	TestConfiguration*		
UpdateTestSuite	Concede permiso para actualizar un conjunto de pruebas	Escritura	TestSuite*		

Tipos de recursos definidos por las Pruebas de aplicaciones de AWS Mainframe Modernizations

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
TestCase	`arn:${Partition}:apptest:${Region}:${Account}:testcase/${TestCaseId}`	aws:ResourceTag/${TagKey}
TestConfiguration	`arn:${Partition}:apptest:${Region}:${Account}:testconfiguration/${TestConfigurationId}`	aws:ResourceTag/${TagKey}
TestRun	`arn:${Partition}:apptest:${Region}:${Account}:testrun/${TestRunId}`	aws:ResourceTag/${TagKey}
TestSuite	`arn:${Partition}:apptest:${Region}:${Account}:testsuite/${TestSuiteId}`	aws:ResourceTag/${TagKey}

Claves de condición para las Pruebas de aplicaciones de AWS Mainframe Modernization

AWS Las pruebas de aplicaciones de modernización del mainframe definen las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Mainframe Modernization Service

AWS El Servicio de Modernización de Mainframe (prefijo de servicio:`m2`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Mainframe Modernization Service
- Tipos de recursos definidos por AWS Mainframe Modernization Service
- Claves de condición para AWS Mainframe Modernization Service

Acciones definidas por AWS Mainframe Modernization Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelBatchJobExecution	Otorga permiso para cancelar la ejecución de un trabajo por lotes	Escritura	Application*		
CreateApplication	Concede permiso para crear una aplicación.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateDataSetExportTask	Otorga permiso para crear una tarea de exportación de conjuntos de datos	Escritura	Application*		s3:GetObject
CreateDataSetImportTask	Otorga permiso para crear una tarea de importación de conjuntos de datos	Escritura	Application*		s3:GetObject
CreateDeployment	Concede permiso para crear una implementación.	Escritura	Application*		elasticloadbalancing:AddTags elasticloadbalancing:CreateListener elasticloadbalanci

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ng:CreateTargetGroup elasticloadbalancing:RegisterTargets
			Environment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironment	Otorga permiso para crear un entorno	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					elasticfilesystem:DescribeMountTargets elasticloadbalancing:AddTags elasticloadbalancing:CreateLoadBalancer fsx:DescribeFileSystems iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApplication	Concede permiso para eliminar una aplicación.	Escritura	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteApplicationFromEnvironment	Otorga permiso para eliminar una aplicación de un entorno de tiempo de ejecución	Escritura	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteEnvironment	Otorga permiso para eliminar un entorno de tiempo de ejecución	Escritura	Environment*		elasticloadbalancing:DeleteLoadBalancer
GetApplication	Otorga permiso para recuperar una aplicación	Lectura	Application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetApplicationVersion	Otorga permiso para recuperar la versión de una aplicación	Lectura	Application*		
GetBatchJobExecution	Otorga permiso para recuperar la ejecución de un trabajo por lotes	Lectura	Application*		
GetDataSetDetails	Otorga permiso para recuperar detalles de un conjunto de datos	Lectura	Application*		
GetDataSetExportTask	Otorga permiso para exportar un conjunto de datos en la ubicación S3 especificada	Lectura	Application*		
GetDataSetImportTask	Otorga permiso para recuperar una tarea de importación de conjuntos de datos	Lectura	Application*		
GetDeployment	Otorga permiso para recuperar una implementación	Lectura	Application*		
GetEnvironment	Otorga permiso para recuperar un entorno de tiempo de ejecución	Lectura	Environment*		
GetSignedBluinsightsUrl	Concede permiso para crear una URL de Bluinsights firmada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApplicationVersions	Otorga permiso para obtener una lista de versiones de una aplicación	Lectura	Application*		
ListApplications	Concede permiso para enumerar las aplicaciones.	Enumeración			
ListBatchJobDefinitions	Otorga permiso para enumerar definiciones de trabajo por lotes	Lectura	Application*		
ListBatchJobExecutions	Otorga permiso para enumerar las ejecuciones de un trabajo por lotes	Lectura	Application*		
ListBatchJobRestartPoints	Otorga permiso para recuperar la ejecución de un trabajo por lotes	Lectura	Application*		
ListDataSetExportHistory	Otorga permiso para enumerar el historial de exportación del conjunto de datos	Lectura	Application*		
ListDataSetImportHistory	Otorga permiso para enumerar el historial importación de conjuntos de datos	Lectura	Application*		
ListDataSets	Otorga permiso para enumerar conjuntos de datos	Lectura	Application*		
ListDeployments	Otorga permiso para enumerar implementaciones	Lectura	Application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEngineVersions	Otorga permiso para enumerar las versiones del motor	Lectura			
ListEnvironments	Otorga permiso para enumerar los entornos de tiempo de ejecución	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
StartApplication	Otorga permiso para iniciar una aplicación	Escritura	Application*		
StartBatchJob	Otorga permisos para comenzar un trabajo por lotes	Escritura	Application*		
StopApplication	Otorga permiso para detener una aplicación	Escritura	Application*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	Application		
			Environment		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	Application		
			Environment		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	Application*		s3:GetObject s3:ListBucket
UpdateEnvironment	Otorga permiso para actualizar un entorno de tiempo de ejecución	Escritura	Environment*		

Tipos de recursos definidos por AWS Mainframe Modernization Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Application	`arn:${Partition}:m2:${Region}:${Account}:app/${ApplicationId}`	aws:ResourceTag/${TagKey}
Environment	`arn:${Partition}:m2:${Region}:${Account}:env/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Mainframe Modernization Service

AWS El Servicio de Modernización de Mainframe define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Managed Blockchain

Amazon Managed Blockchain (prefijo de servicio: `managedblockchain`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Blockchain
- Tipos de recursos definidos por Amazon Managed Blockchain
- Claves de condición para Amazon Managed Blockchain

Acciones definidas por Amazon Managed Blockchain

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccessor	Otorga permiso para crear un acceso Amazon Managed Blockchain	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMember	Otorga permiso para crear un miembro de una red Amazon Managed Blockchain	Write	network*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetwork	Otorga permiso para crear una red Amazon Managed Blockchain	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateNode	Otorga permiso para crear un nodo en un miembro de una red Amazon Managed Blockchain	Write	member		iam:CreateServiceLinkedRole
			network		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProposal	Otorga permiso para crear una propuesta que otros miembros de la red de cadena de bloques pueden votar para agregar o eliminar a un miembro de una red Amazon Managed Blockchain.	Escritura	network*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccessor	Otorga permiso para eliminar un acceso Amazon Managed Blockchain	Escritura	accessor*		
DeleteMember	Otorga permiso para eliminar a un miembro y todos los recursos asociados de una red Amazon Managed Blockchain	Write	member*		
DeleteNode	Otorga permiso para eliminar un nodo de un miembro de una red Amazon Managed Blockchain	Escritura	node*		
GET [solo permiso]	Otorga permiso para enviar solicitudes HTTP GET a un nodo Ethereum	Administración de permisos			
GetAccessor	Otorga permiso para devolver información detallada sobre un acceso Amazon Managed Blockchain	Lectura	accessor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMember	Otorga permiso para devolver información detallada sobre un miembro de una red Amazon Managed Blockchain	Read	member*		
GetNetwork	Otorga permiso para devolver información detallada sobre una red Amazon Managed Blockchain	Read	network*		
GetNode	Otorga permiso para devolver información detallada sobre un nodo de un miembro de una red Amazon Managed Blockchain	Read	node*		
GetProposal	Otorga permiso para devolver información detallada sobre una propuesta de una red Amazon Managed Blockchain	Lectura	proposal*		
Invoke [solo permiso]	Otorga permiso para crear WebSocket conexiones a un nodo de Ethereum	Administración de permisos			
InvokeRpcBitcoinMainnet	Otorga permiso para invocar la red principal de Bitcoin RPCs	Lectura			
InvokeRpcBitcoinTestnet	Otorga permiso para invocar la red de pruebas de Bitcoin RPCs	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InvokeRpcPolygonMainnet	Otorga permiso para invocar la red principal de Polygon RPCs	Lectura			
InvokeRpcPolygonMumbaiTestnet	Otorga permiso para invocar la red de pruebas de Polygon Mumbai RPCs	Lectura			
ListAccessors	Otorga permiso para enumerar los accesores de Amazon Managed Blockchain propiedad del usuario actual Cuenta de AWS	Enumeración			
ListInvitations	Otorga permiso para enumerar las invitaciones extendidas al activo Cuenta de AWS desde cualquier red de cadena de bloques gestionada	Enumeración			
ListMembers	Otorga permiso para enumerar los miembros de una red Amazon Managed Blockchain y las propiedades de las suscripciones	Enumeración	network*		
ListNetworks	Otorga permiso para enumerar las redes Amazon Managed Blockchain en las que Cuenta de AWS participa actualmente	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNodes	Otorga permiso para crear una lista de los nodos de un miembro de una red Amazon Managed Blockchain	List	member		
			network		
ListProposalVotes	Otorga permiso para crear una lista de todos los votos para una propuesta, incluido el valor del voto y el identificador único del miembro que ha dado el voto a la red Amazon Managed Blockchain	Read	proposal*		
ListProposals	Otorga permiso para crear una lista de propuestas para la red Amazon Managed Blockchain determinada	List	network*		
ListTagsForResource	Otorga permiso para ver etiquetas asociadas a un recurso de Amazon Managed Blockchain	Lectura	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
POST [solo permiso]	Otorga permiso para enviar solicitudes HTTP POST a un nodo Ethereum	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RejectInvitation	Concede permiso para rechazar la invitación para unirse a la red de cadena de bloques	Write	invitation*		
TagResource	Otorga permiso para agregar etiquetas a un recurso de Amazon Managed Blockchain	Etiquetado	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de Amazon Managed Blockchain	Etiquetado	accessor		
			invitation		
			member		
			network		
			node		
			proposal		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateMember	Otorga permiso para actualizar un miembro de una red Amazon Managed Blockchain	Write	member*		iam:CreateServiceLinkedRole
UpdateNode	Otorga permiso para actualizar un nodo de un miembro de una red Amazon Managed Blockchain	Write	node*		iam:CreateServiceLinkedRole
VoteOnProposal	Otorga permiso para votar a una propuesta en nombre del miembro de la red de cadena de bloques especificado	Write	proposal*		

Tipos de recursos definidos por Amazon Managed Blockchain

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
network	`arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
member	arn:${Partition}:managedblockchain:${Region}:${Account}:members/${MemberId}	aws:ResourceTag/${TagKey}
node	arn:${Partition}:managedblockchain:${Region}:${Account}:nodes/${NodeId}	aws:ResourceTag/${TagKey}
proposal	arn:${Partition}:managedblockchain:${Region}::proposals/${ProposalId}	aws:ResourceTag/${TagKey}
invitation	arn:${Partition}:managedblockchain:${Region}:${Account}:invitations/${InvitationId}	aws:ResourceTag/${TagKey}
accessor	arn:${Partition}:managedblockchain:${Region}:${Account}:accessors/${AccessorId}	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Managed Blockchain

Amazon Managed Blockchain define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de las etiquetas asociadas a un recurso de Amazon Managed Blockchain	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Managed Blockchain Query

Amazon Managed Blockchain Query (prefijo de servicio: `managedblockchain-query`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Blockchain Query
- Tipos de recursos definidos por Amazon Managed Blockchain Query
- Claves de condición para Amazon Managed Blockchain Query

Acciones definidas por Amazon Managed Blockchain Query

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetTokenBalance	Otorga permiso para agrupar las llamadas a la API GetTokenBalance	Lectura			
GetAssetContract	Concede permiso para obtener información sobre un contrato de la cadena de bloques	Lectura			
GetTokenBalance	Otorga permiso para recuperar el saldo de un token para una dirección en la cadena de bloques	Lectura			
GetTransaction	Otorga permiso para recuperar una transacción en la cadena de bloques	Lectura			
ListAssetContracts	Concede permiso para recuperar varios contratos de la cadena de bloques	Enumeración			
ListFilteredTransactionEvents	Concede permiso para recuperar eventos en la cadena de bloques con filtros adicionales	Enumeración			
ListTokenBalances	Otorga permiso para recuperar múltiples saldos en la cadena de bloques	Enumeración			
ListTransactionEvents	Otorga permiso para recuperar eventos en una	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	transacción en la cadena de bloques				
ListTransactions	Otorga permiso para recuperar múltiples transacciones en una cadena de bloques	Enumeración			

Tipos de recursos definidos por Amazon Managed Blockchain Query

Amazon Managed Blockchain Query no admite la especificación de un ARN de recurso en el elemento de `Resource` de una declaración de política de IAM. Para permitir el acceso a Amazon Managed Blockchain Query, especifique `"Resource": "*"` en su política.

Claves de condición para Amazon Managed Blockchain Query

Managed Blockchain no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condiciones AWS globales.

Acciones, recursos y claves de condición para Amazon Managed Grafana

Amazon Managed Grafana (prefijo de servicio: `grafana`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para usarlos en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Grafana
- Tipos de recursos definidos por Amazon Managed Grafana
- Claves de condición de Amazon Managed Grafana

Acciones definidas por Amazon Managed Grafana

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateLicense	Concede permiso para actualizar un espacio de trabajo con una licencia	Write	workspace*		aws-marketplace:ViewSubscriptions
CreateWorkspace	Concede permiso para crear un espacio de trabajo	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceL

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					inkedRole organizations:DescribeOrganization sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions sso:GetSharedSsoConfiguration
CreateWorkspaceApiKey	Concede permiso para crear claves de API para un espacio de trabajo	Escritura	workspace*		
CreateWorkspaceServiceAccount	Concede permiso para crear cuentas de servicio para un espacio de trabajo	Escritura	workspace*		
CreateWorkspaceServiceAccountToken	Concede permiso para crear tokens de cuenta de servicio de un espacio de trabajo	Escritura	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteWorkspace	Concede permiso para eliminar un espacio de trabajo	Escritura	workspace*		sso:DeleteManagedApplicationInstance
DeleteWorkspaceApiKey	Concede permiso para eliminar claves de API de un espacio de trabajo	Escritura	workspace*		
DeleteWorkspaceServiceAccount	Concede permiso para eliminar cuentas de servicio de un espacio de trabajo.	Escritura	workspace*		
DeleteWorkspaceServiceAccountToken	Concede permiso para eliminar tokens de cuenta de servicio de un espacio de trabajo	Escritura	workspace*		
DescribeWorkspace	Concede permiso para describir un espacio de trabajo	Lectura	workspace*		
DescribeWorkspaceAuthentication	Concede permiso para describir los proveedores de autenticación en un espacio de trabajo	Lectura	workspace*		
DescribeWorkspaceConfiguration	Otorga permiso para describir la cadena de configuración actual para el espacio de trabajo predeterminado	Lectura	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateLicense	Concede permiso para quitar una licencia de un espacio de trabajo	Write	workspace*		
ListPermissions	Concede permiso para enumerar los permisos de un espacio de trabajo	Enumeración	workspace*		
ListTagsForResource	Concede permiso para mostrar la lista de las etiquetas asociadas a un espacio de trabajo	Lectura	workspace		
ListVersions	Otorga permiso para enumerar todas las versiones compatibles de Grafana disponibles. Si lo desea, incluya un espacio de trabajo para enumerar las versiones a las que se puede actualizar	Enumeración	workspace		
ListWorkspaceServiceAccountTokens	Concede permiso para enumerar tokens de cuenta de servicio de un espacio de trabajo	Lectura	workspace*		
ListWorkspaceServiceAccounts	Concede permiso para enumerar cuentas de servicio de un espacio de trabajo	Lectura	workspace*		
ListWorkspaces	Concede permiso para enumerar los espacios de trabajo	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para agregar etiquetas o actualizar valores de etiqueta de un espacio de trabajo	Etiquetado	workspace*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para quitar etiquetas de un espacio de trabajo	Etiquetado	workspace*		
				aws:TagKeys	
UpdatePermissions	Concede permiso para modificar los permisos de un espacio de trabajo	Permissions management	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateWorkspace	Concede permiso para modificar un espacio de trabajo.	Escritura	workspace*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole
UpdateWorkspaceAuthentication	Concede permiso para modificar los proveedores de autenticación en un espacio de trabajo	Escritura	workspace*		
UpdateWorkspaceConfiguration	Otorga permiso para actualizar la cadena de configuración para el espacio de trabajo predeterminado.	Escritura	workspace*		

Tipos de recursos definidos por Amazon Managed Grafana

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
workspace	`arn:${Partition}:grafana:${Region}:${Account}:/workspaces/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Managed Grafana

Amazon Managed Grafana define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante acciones en función de pares de clave-valor asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante acciones en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus (prefijo de servicio: `aps`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Service for Prometheus
- Tipos de recursos definidos por Amazon Managed Service for Prometheus
- Claves de condición de Amazon Managed Service for Prometheus

Acciones definidas por Amazon Managed Service for Prometheus

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAlertManagerAlerts	Otorga permiso para crear alertas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAlertManagerDefinition	Otorga permiso para crear una definición de administrador de alertas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
CreateLoggingConfiguration	Concede permiso para crear una configuración de registro.	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
CreateQueryLoggingConfiguration	Otorga permiso para crear una configuración de registro de consultas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
CreateRuleGroupsNamespace	Otorga permiso para crear un espacio de nombres de grupos de reglas	Escritura	rulegroupsnamespace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateScraper	Concede permiso para crear un scraper	Escritura	cluster*		aps:TagResource ec2:DescribeSecurityGroups ec2:DescribeSubnets eks:DescribeCluster iam:CreateServiceLinkedRole
			workspace*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateWorkspace	Concede permiso para crear un espacio de trabajo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlertManagerDefinition	Otorga permiso para eliminar una definición de administrador de alertas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteAlertManagerSilence	Otorga permiso para eliminar un silencio	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteLoggingConfiguration	Concede permiso para eliminar una configuración de registro.	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteQueryLoggingConfiguration	Otorga permiso para eliminar una configuración de registro de consultas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRuleGroupsNamespace	Otorga permiso para eliminar un espacio de nombres de grupos de reglas	Escritura	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DeleteScraper	Concede permiso para eliminar un scraper	Escritura	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteWorkspace	Concede permiso para eliminar un espacio de trabajo	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeAlertManagerDefinition	Otorga permiso para describir una definición de administrador de alertas	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingConfiguration	Concede permiso para describir una configuración de registro.	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeQueryLoggingConfiguration	Otorga permiso para describir una configuración de registro de consultas	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeRuleGroupsNamespace	Otorga permiso para describir un espacio de nombres de grupos de reglas	Lectura	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DescribeScraper	Concede permiso para describir un scraper	Lectura	scraper*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspace	Concede permiso para describir un espacio de trabajo	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceConfiguration	Otorga permiso para describir la configuración del espacio de trabajo	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAlertManagerSilence	Otorga permiso para obtener un silencio	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerStatus	Otorga permiso para obtener el estado actual de un administrador de alertas	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
GetDefaultScraperConfiguration	Concede permiso para obtener la configuración de scraper predeterminada	Lectura			
GetLabels	Otorga permiso para recuperar las etiquetas de un espacio de trabajo de AMP	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetMetricMetadata	Otorga permiso para recuperar los metadatos de las métricas del espacio de trabajo de AMP	Read	workspace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSeries	Otorga permiso para recuperar los datos de series temporales del espacio de trabajo de AMP	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlertGroups	Otorga permiso para enumerar grupos	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlerts	Otorga permiso para enumerar alertas	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerReceivers	Otorga permiso para enumerar receptores	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerSilences	Otorga permiso para obtener silencios	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAlerts	Otorga permiso para enumerar alertas activas	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
ListRuleGroupsNamespaces	Otorga permiso para enumerar los espacios de nombres de grupos de reglas	Enumeración	workspace*		
				aws:ResourceTag/${TagKey}	
ListRules	Otorga permiso para enumerar las reglas de registro y alerta	Lectura	workspace*		
				aws:ResourceTag/${TagKey}	
ListScrapers	Concede permiso para enumerar scrapers	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas para un recurso AMP	Lectura	rulegroupsnamespace		
			scraper		
			workspace		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
ListWorkspaces	Otorga permiso para enumerar los espacios de trabajo	Enumeración			
PutAlertManagerDefinition	Otorga permiso para actualizar una definición de administrador de alertas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerSilences	Otorga permiso para crear o actualizar un silencio	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
PutRuleGroupsNamespace	Otorga permiso para actualizar un espacio de nombres de grupos de reglas	Escritura	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
QueryMetrics	Concede permiso para ejecutar una consulta en las métricas de espacio de trabajo de AMP	Read	workspace*		
				aws:ResourceTag/${TagKey}	
RemoteWrite	Otorga permiso para realizar una operación de escritura remota para iniciar la transmisión de métricas al espacio de trabajo de AMP	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
TagResource	Otorga permiso para etiquetar un recurso de AMP	Etiquetado	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para desetiquetar un recurso de AMP	Etiquetado	rulegroupsnamespace		
			scraper		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workspace		
				aws:TagKeys	
UpdateLoggingConfiguration	Concede permiso para actualizar una configuración de registro.	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateQueryLoggingConfiguration	Otorga permiso para actualizar una configuración de registro de consultas	Escritura	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateScraper	Otorga permiso para actualizar un raspador	Escritura	scraper*		aps:CreateScraper aps:TagResource
			workspace		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceAlias	Otorga permiso para modificar el alias del espacio de trabajo de AMP existente	Escritura	workspace*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceConfiguration	Otorga permiso para actualizar la configuración del espacio de trabajo	Escritura	workspace *		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon Managed Service for Prometheus

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
workspace	`arn:${Partition}:aps:${Region}:${Account}:workspace/${WorkspaceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Tipos de recurso	ARN	Claves de condición
rulegroupsnamespace	`arn:${Partition}:aps:${Region}:${Account}:rulegroupsnamespace/${WorkspaceId}/${Namespace}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
scraper	`arn:${Partition}:aps:${Region}:${Account}:scraper/${ScraperId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Managed Service for Prometheus

Amazon Managed Service para Prometheus define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Managed Streaming for Apache Kafka.

Amazon Managed Streaming for Apache Kafka (prefijo de servicio: `kafka`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Streaming for Apache Kafka.
- Tipos de recurso definidos por Amazon Managed Streaming for Apache Kafka.
- Claves de condición de Amazon Managed Streaming for Apache Kafka.

Acciones definidas por Amazon Managed Streaming for Apache Kafka.

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchAssociateScramSecret	Otorga permiso para asociar uno o más secretos de Scram con un clúster de Amazon MSK	Write	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Otorga permiso para disociar uno o más secretos de Scram de un clúster de Amazon MSK.	Write	cluster*		kms:RetireGrant
CreateCluster	Otorga permiso para crear un clúster de MSK	Escritura	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateClusterV2	Otorga permiso para crear un clúster de MSK	Write	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Otorga permiso para crear una configuración de MSK	Escritura	configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateReplicator	Concede permiso para crear un replicador de MSK	Escritura	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVpcConnection	Concede permiso para crear una conexión de VPC de MSK	Escritura	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Otorga permiso para eliminar un clúster de MSK	Escritura	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	Concede permiso para eliminar una política basada en recursos de un clúster	Escritura	cluster*		
DeleteConfiguration	Otorga permiso para eliminar la configuración de MSK especificada	Escritura	configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteReplicator	Concede permiso para eliminar un replicador de MSK	Escritura	replicator*		
DeleteVpcConnection	Concede permiso para eliminar una conexión de VPC de MSK	Escritura	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	Otorga permiso para describir un clúster de MSK	Read	cluster*		
DescribeClusterOperation	Otorga permiso para describir la operación de clúster especificada por el ARN dado	Lectura			
DescribeClusterOperationV2	Otorga permiso para describir la operación de clúster especificada por el ARN dado	Lectura			
DescribeClusterV2	Otorga permiso para describir un clúster de MSK	Lectura	cluster*		
DescribeConfiguration	Otorga permiso para describir una configuración de MSK	Read	configuration*		
DescribeConfigurationRevision	Otorga permiso para describir la revisión de una configuración de MSK	Lectura	configuration*		
DescribeReplicator	Concede permiso para describir un replicador de MSK	Lectura	replicator*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeVpcConnection	Concede permiso para describir una conexión de VPC de MSK	Lectura	vpc-connection*		
GetBootstrapBrokers	Otorga permiso para obtener los detalles de conexión de los agentes de un clúster de MSK	Lectura			
GetClusterPolicy	Concede permiso para describir una política basada en recursos de un clúster	Lectura	cluster*		
GetCompatibleKafkaVersions	Otorga permiso para obtener una lista de las versiones de Apache Kafka a las que puede actualizar un clúster de MSK	Enumeración			
ListClientVpcConnections	Concede permiso para enumerar todas las conexiones de VPC de MSK creadas para un clúster	Enumeración	cluster*		
ListClusterOperations	Otorga permiso para devolver una lista de todas las operaciones que se han llevado a cabo en el clúster especificado de MSK	Enumeración	cluster*		
ListClusterOperationsV2	Otorga permiso para devolver una lista de todas las operaciones que se han llevado a cabo en el clúster especificado de MSK	List	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListClusters	Otorga permiso para enumerar todos los clústeres de MSK de esta cuenta	Enumeración			
ListClustersV2	Otorga permiso para enumerar todos los clústeres de MSK de esta cuenta	List			
ListConfigurationRevisions	Otorga permiso para enumerar todas las revisiones de una configuración de MSK de esta cuenta	List	configuration*		
ListConfigurations	Otorga permiso para enumerar todas las configuraciones de MSK de esta cuenta	List			
ListKafkaVersions	Otorga permiso para enumerar todas las versiones de Apache Kafka compatibles con Amazon MSK	List			
ListNodes	Otorga permiso para enumerar los agentes de un clúster de MSK	Enumeración	cluster*		
ListReplicators	Concede permiso para enumerar todos los replicadores de MSK de esta cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListScramSecrets	Otorga permiso para enumerar los secretos de Scram asociados a un clúster de Amazon MSK	List	cluster*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso de MSK	Lectura	cluster*		
ListVpcConnections	Concede permiso para enumerar todas las conexiones de VPC de MSK que utiliza esta cuenta	Enumeración			
PutClusterPolicy	Concede permiso para crear o actualizar la política basada en recursos de un clúster	Escritura	cluster*		
RebootBroker	Otorga permiso para reiniciar un agente	Escritura	cluster*		
RejectClientVpcConnection	Concede permiso para rechazar una conexión de VPC de MSK	Escritura	cluster* vpc-connection*		
TagResource	Otorga permiso para etiquetar un recurso de MSK	Etiquetado	cluster vpc-connection		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar las etiquetas de un recurso de MSK	Etiquetado	cluster		
			vpc-connection		
				aws:TagKeys	
UpdateBrokerCount	Otorga permiso para actualizar la cantidad de agentes del clúster de MSK	Write	cluster*		
UpdateBrokerStorage	Otorga permiso para actualizar el tamaño de almacenamiento de los agentes del clúster de MSK	Write	cluster*		
UpdateBrokerType	Otorga permiso para actualizar el tipo de agente de un clúster de Amazon MSK	Write	cluster*		
UpdateClusterConfiguration	Otorga permiso para actualizar la configuración del clúster de MSK	Write	cluster*		
			configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateClusterKafkaVersion	Otorga permiso para actualizar el clúster de MSK a la versión de Apache Kafka especificada	Write	cluster*		
UpdateConfiguration	Otorga permiso para crear una nueva revisión de la configuración de MSK	Escritura	configuration*		
UpdateConnectivity	Otorga permiso para actualizar la configuración de conectividad del clúster de MSK.	Escritura	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets
				kafka:publicAccessEnabled	
UpdateMonitoring	Otorga permiso para actualizar la configuración de monitoreo del clúster de MSK	Escritura	cluster*		
UpdateReplicationInfo	Concede permiso para actualizar la información de replicación del replicador de MSK	Escritura	replicator*		
UpdateSecurity	Otorga permiso para actualizar la configuración de seguridad del clúster de MSK	Escritura	cluster*		kms:RetireGrant

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateStorage	Concede permiso para actualizar el almacenamiento de EBS (tamaño o rendimiento aprovisionado) asociado a los agentes de MSK o establecer el modo de almacenamiento en clúster como TIERED	Escritura	cluster*		

Tipos de recurso definidos por Amazon Managed Streaming for Apache Kafka.

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}
configuration	`arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}`	
vpc-connection	`arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${Clu`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
	sterOwnerAccount}/${ClusterName}/${Uuid}	
replicator	arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Claves de condición de Amazon Managed Streaming for Apache Kafka.

Amazon Managed Streaming for Apache Kafka define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
kafka:publicAccessEnabled	Filtra el acceso en función de la presencia de acceso público habilitado en la solicitud	Bool

Acciones, recursos y claves de condición para Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming for Kafka Connect (prefijo de servicio: `kafkaconnect`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Streaming for Kafka Connect
- Tipos de recurso definidos por Amazon Managed Streaming for Kafka Connect
- Claves de condición de Amazon Managed Streaming for Kafka Connect

Acciones definidas por Amazon Managed Streaming for Kafka Connect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnector	Otorga permiso para crear un conector de MSK Connect	Escritura			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs firehose:TagDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:PutRolePolicy logs:CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy s3:GetBucketPolicy s3:PutBucketPolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCustomPlugin	Otorga permiso para crear un complemento a medida de MSK Connect	Escritura			s3:GetObject
CreateWorkerConfiguration	Otorga permiso para crear una configuración de empleado de MSK Connect	Escritura			
DeleteConnector	Otorga permiso para eliminar un conector de MSK Connect	Escritura	connector*		logs:DeleteLogDelivery logs:ListLogDeliveries
DeleteCustomPlugin	Concede permiso para eliminar un complemento a medida de MSK Connect	Escritura	custom plugin*		
DeleteWorkerConfiguration	Concede permiso para eliminar una configuración de empleado de MSK Connect	Escritura	worker configuration*		
DescribeConnector	Otorga permiso para describir un conector de MSK Connect	Lectura	connector*		
DescribeConnectorOperation	Otorga permiso para describir el funcionamiento de un conector MSK Connect	Lectura	connector operation*		
DescribeCustomPlugin	Otorga permiso para describir un complemento a medida de MSK Connect	Lectura	custom plugin*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeWorkerConfiguration	Otorga permiso para describir una configuración de empleado de MSK Connect	Lectura	worker configuration*		
ListConnectorOperations	Otorga permiso para enumerar todas las operaciones de un conector MSK Connect determinado	Lectura	connector*		
ListConnectors	Otorga permiso para enumerar todos los conectores de MSK Connect de esta cuenta	Lectura			
ListCustomPlugins	Otorga permiso para enumerar todos los complementos a medida de MSK Connect de esta cuenta	Lectura			
ListTagsForResource	Concede permiso para enumerar etiquetas de un recurso de MSK Connect	Lectura	connector	aws:ResourceTag/${TagKey}	
			custom plugin	aws:ResourceTag/${TagKey}	
			worker configuration	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorkerConfigurations	Otorga permiso para enumerar todas las configuraciones de empleado de MSK Connect de esta cuenta	Lectura			
TagResource	Concede permiso para etiquetar un recurso de MSK Connect	Etiquetado	connector	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			custom plugin	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			worker configuration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso de MSK Connect	Etiquetado	connector	aws:TagKeys	
			custom plugin	aws:TagKeys	
			worker configuration	aws:TagKeys	
				aws:TagKeys	
UpdateConnector	Otorga permiso para actualizar un conector de MSK Connect	Escritura	connector *		

Tipos de recurso definidos por Amazon Managed Streaming for Kafka Connect

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
connector	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector/${ConnectorName}/${UUID}`	aws:ResourceTag/${TagKey}
custom plugin	`arn:${Partition}:kafkaconnect:${Region}:${Account}:custom-plugin/${CustomPluginName}/${UUID}`	aws:ResourceTag/${TagKey}
worker configuration	`arn:${Partition}:kafkaconnect:${Region}:${Account}:worker-configuration/${WorkerConfigurationName}/${UUID}`	aws:ResourceTag/${TagKey}
connector operation	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector-operation/${ConnectorName}/${ConnectorUUID}/${UUID}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming para Kafka Connect define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow (prefijo de servicio: `airflow`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Managed Workflows for Apache Airflow
- Tipos de recursos definidos por Amazon Managed Workflows for Apache Airflow
- Claves de condición de Amazon Managed Workflows for Apache Airflow

Acciones definidas por Amazon Managed Workflows for Apache Airflow

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCliToken	Otorga permiso para crear un token de corta duración que permita al usuario invocar la CLI de Airflow a través de un punto de enlace del servidor web de Apache Airflow	Write	environment*		
CreateEnvironment	Otorga permiso para crear un entorno de Amazon MWAA	Write	environment*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebLoginToken	Otorga permiso para crear un token de corta duración que permita al usuario iniciar sesión en la interfaz de usuario web de Apache Airflow	Write	rbac-role*		
DeleteEnvironment	Otorga permiso para eliminar un entorno de Amazon MWAA	Write	environment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetEnvironment	Otorga permiso para ver los detalles de un entorno de Amazon MWAA	Lectura	environment*		
				aws:ResourceTag/${TagKey}	
InvokeRestApi	Concede permiso para invocar la API de REST de Airflow a través de un punto de conexión en el servidor web de Apache Airflow	Escritura	rbac-role*		
ListEnvironments	Otorga permiso para enumerar los entornos de Amazon MWAA de su cuenta	List			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un entorno de Amazon MWAA	Read	environment		
				aws:ResourceTag/${TagKey}	
PublishMetrics	Otorga permiso para publicar las métricas de un entorno de Amazon MWAA	Write	environment*		
TagResource	Otorga permiso para etiquetar un entorno de Amazon MWAA	Etiquetado	environment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para quitar las etiquetas de un entorno de Amazon MWAA	Etiquetado	environment		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Otorga permiso para modificar un entorno de Amazon MWAA	Write	environment*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon Managed Workflows for Apache Airflow

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment	`arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}`	
rbac-role	`arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}`	

Claves de condición de Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Marketplace

AWS Marketplace (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace
- Tipos de recursos definidos por AWS Marketplace
- Claves de condición de AWS Marketplace

Acciones definidas por AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptAgreementApprovalRequest	Permite a los usuarios aprobar una solicitud de suscripción entrante (para proveedores que proporcionan productos que requieren verificación de suscripción)	Escritura			
AcceptAgreementRequest	Otorga permiso a los usuarios para aceptar sus solicitudes de contrato. Debe tenerse en	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	cuenta que esta acción no se aplica a las compras en Marketplace				
CancelAgreement	Otorga permiso a los usuarios para cancelar sus contratos Debe tenerse en cuenta que esta acción no se aplica a las compras en Marketplace	Escritura			
CancelAgreementRequest	Permite a los usuarios cancelar solicitudes de suscripción pendientes para productos que requieren verificación de suscripción	Escritura			
CreateAgreementRequest	Otorga permiso a los usuarios para crear una solicitud de contrato. Debe tenerse en cuenta que esta acción no se aplica a las compras en Marketplace	Escritura			
DescribeAgreement	Permite a los usuarios describir los metadatos sobre el contrato	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAgreementApprovalRequest	Permite a los usuarios ver información detallada de sus solicitudes de suscripción entrantes (para proveedores que proporcionan productos que requieren verificación de suscripción)	Lectura			
GetAgreementEntitlements	Otorga permiso a los usuarios para ver los derechos asociados a un acuerdo	Lectura			
GetAgreementRequest	Permite a los usuarios ver los detalles de sus solicitudes de suscripción para productos de datos que requieren verificación de suscripción	Lectura			
GetAgreementTerms	Otorga permiso a los usuarios para obtener una lista de términos para un contrato	Enumeración			
ListAgreementApprovalRequests	Permite a los usuarios crear una lista de sus solicitudes de suscripción entrantes (para proveedores que proporcionan productos que requieren verificación de suscripción)	Enumeración			
ListAgreementCharges	Otorga permiso a los usuarios para ver los cargos asociados a sus acuerdos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAgreementRequests	Permite a los usuarios crear una lista de sus solicitudes de suscripción para productos que requieren verificación de suscripción	Enumeración			
ListEntitlementDetails	Concede permiso a los usuarios para ver los detalles de los derechos asociados a un acuerdo. Debe tenerse en cuenta que esta acción no se aplica a las compras en Marketplace	Lectura			
RejectAgreementApprovalRequest	Permite a los usuarios rechazar solicitudes de suscripción entrantes (para proveedores que proporcionan productos que requieren verificación de suscripción)	Escritura			
SearchAgreements	Permite a los usuarios para buscar sus contratos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Subscribe	Concede permiso a los usuarios para suscribirse a AWS Marketplace los productos. Incluye la posibilidad de enviar una solicitud de suscripción para productos que requieren verificación de suscripción. Incluye la posibilidad de habilitar la renovación automática de una suscripción existente	Escritura			
Unsubscribe	Concede permiso a los usuarios para eliminar las suscripciones a AWS Marketplace los productos. Incluye la posibilidad de desactivar la renovación automática de una suscripción existente	Escritura			
UpdateAgreementApprovalRequest	Permite a los usuarios realizar cambios en una solicitud de suscripción entrante, incluida la posibilidad de eliminar la información del suscriptor potencial (para los proveedores que proporcionan productos que requieren la verificación de la suscripción)	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePurchaseOrders	Concede permiso a los usuarios para actualizar las órdenes de compra para cubrir los cargos asociados a sus acuerdos	Escritura			
ViewSubscriptions	Permite a los usuarios ver las suscripciones de su cuenta	Enumeración			

Tipos de recursos definidos por AWS Marketplace

AWS Marketplace no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Marketplace, especifique `"Resource": "*"` en su política.

Claves de condición de AWS Marketplace

AWS Marketplace define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws-marketplace:AgreementType	Filtra el acceso en función del tipo de contrato	ArrayOfString

Claves de condición	Descripción	Tipo
aws-marketplace:PartyType	Filtra el acceso en función del tipo de parte del contrato	Cadena
aws-marketplace:ProductId	Filtra el acceso por identificador de producto para AWS Marketplace RedHat OpenShift los productos Bedrock. Nota: El uso de esta clave de condición no restringirá el acceso a los productos en AWS Marketplace	ArrayOfString

Acciones, recursos y claves de condición para AWS Marketplace Catalog

AWS Marketplace El catálogo (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace Catalog
- Tipos de recursos definidos por AWS Marketplace Catalog
- Claves de condición para AWS Marketplace Catalog

Acciones definidas por AWS Marketplace Catalog

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelChangeSet	Otorga permiso para cancelar un conjunto de cambios en ejecución	Escritura	ChangeSet*		
DeleteResourcePolicy	Concede permiso para eliminar la política de recursos de una entidad existente	Administración de permisos	Entity*		
DescribeAssessment	Concede permiso para devolver los datos de una evaluación existente	Lectura			
DescribeChangeSet	Otorga permiso para devolver los detalles de un conjunto de cambios existente	Lectura	ChangeSet*		
DescribeEntity	Otorga permiso para devolver los detalles de una entidad existente	Lectura	Entity*		
GetResourcePolicy	Concede permiso para obtener la política de recursos de una entidad existente	Lectura	Entity*		
ListAssessments	Concede permiso para enumerar evaluaciones existentes	Enumeración			
ListChangeSets	Otorga permiso para enumerar los conjuntos de cambios existentes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntities	Otorga permiso para enumerar las entidades existentes	Enumeración			
ListTagsForResource	Otorga permiso para enumerar etiquetas en una entidad existente o en un conjunto de cambios	Lectura	ChangeSet		
			Entity		
PutResourcePolicy	Concede permiso para asociar una política de recursos a una entidad existente	Administración de permisos	Entity*		
StartChangeSet	Otorga permiso para solicitar un nuevo conjunto de cambios (Nota: los permisos a nivel de recursos para esta acción y las claves de contexto de condición para esta acción solo se admiten cuando se usan con la API de catálogo y no se admiten cuando se usan con AWS Marketplace Management Portal)	Escritura	Entity*		
				catalog:ChangeType aws-marketplace:Intent aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Otorga permiso para etiquetar una entidad existente o un conjunto de cambios	Etiquetado	ChangeSet		
			Entity		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar la etiqueta de una entidad existente o de un conjunto de cambios	Etiquetado	ChangeSet		
			Entity		
				aws:TagKeys	

Tipos de recursos definidos por AWS Marketplace Catalog

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType

Tipos de recurso	ARN	Claves de condición
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType

Claves de condición para AWS Marketplace Catalog

AWS Marketplace Catalog define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws-marketplace:Intent	Filtra el acceso según el parámetro de intención de la StartChangeSet solicitud	Cadena
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
catalog:ChangeType	Filtra el acceso por el tipo de cambio de la StartChangeSet solicitud	Cadena

Acciones, recursos y claves de condición para el servicio de análisis de comercio de AWS Marketplace

AWS Marketplace Commerce Analytics Service (prefijo de servicio:`marketplacecommerceanalytics`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

Temas

- Acciones definidas por el servicio de análisis de comercio de AWS Marketplace
- Tipos de recursos definidos por el servicio de análisis de comercio de AWS Marketplace
- Claves de condición para el servicio de análisis de comercio de AWS Marketplace

Acciones definidas por el servicio de análisis de comercio de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateDataSet	Solicita que se publique un conjunto de datos en su bucket de Amazon S3.	Write			
StartSupportDataExport	Solicita que se publique un conjunto de datos de soporte en su bucket de Amazon S3.	Write			

Tipos de recursos definidos por el servicio de análisis de comercio de AWS Marketplace

AWS Marketplace Commerce Analytics Service no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al servicio de análisis de comercio de AWS Marketplace , especifique `"Resource": "*"` en su política.

Claves de condición para el servicio de análisis de comercio de AWS Marketplace

El servicio de análisis de comercio (CAS) no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de la política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el servicio de implementación de AWS Marketplace

AWS Marketplace El servicio de despliegue (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de implementación de AWS Marketplace
- Tipos de recursos definidos por el servicio de implementación de AWS Marketplace
- Claves de condición para el servicio de implementación de AWS Marketplace

Acciones definidas por el servicio de implementación de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso de parámetros de implementación	Lectura	DeploymentParameter		
				aws:ResourceTag/${TagKey}	
PutDeploymentParameter	Concede permiso para crear o actualizar un recurso de parámetros de implementación	Escritura	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	aws-marketplace:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para etiquetar un recurso de parámetros de implementación	Etiquetado	DeploymentParameter*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso de parámetros de implementación	Etiquetado	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por el servicio de implementación de AWS Marketplace

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
DeploymentParameter	`arn:${Partition}:aws-marketplace:${Region}:${Account}:DeploymentParameter:catalogs/${CatalogName}/products/${ProductId}/${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Claves de condición para el servicio de implementación de AWS Marketplace

AWS Marketplace El servicio de despliegue define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Marketplace Discovery

AWS Marketplace Discovery (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace Discovery
- Tipos de recursos definidos por AWS Marketplace Discovery
- Claves de condición para AWS Marketplace Discovery

Acciones definidas por AWS Marketplace Discovery

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPrivateListings	Otorga permiso a los usuarios para enumerar sus ofertas privadas	Enumeración			

Tipos de recursos definidos por AWS Marketplace Discovery

AWS Marketplace Discovery no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Marketplace Discovery, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Marketplace Discovery

Marketplace Discovery no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el servicio de concesión de derechos de AWS Marketplace

AWS Marketplace Entitlement Service (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de concesión de derechos de AWS Marketplace
- Tipos de recursos definidos por el servicio de concesión de derechos de AWS Marketplace
- Claves de condición para el servicio de concesión de derechos de AWS Marketplace

Acciones definidas por el servicio de concesión de derechos de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEntitlements	Concede permiso para recuperar valores de derechos para un producto determinado. Los resultados se pueden filtrar en función del identificador del cliente o de las dimensiones del producto	Read			

Tipos de recursos definidos por el servicio de concesión de derechos de AWS Marketplace

AWS Marketplace Entitlement Service no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al servicio de concesión de derechos de AWS Marketplace , especifique `"Resource": "*"` en su política.

Claves de condición para el servicio de concesión de derechos de AWS Marketplace

La medición de Marketplace Entitlement no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el servicio de compilación de imágenes de AWS Marketplace

AWS Marketplace Image Building Service (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de compilación de imágenes de AWS Marketplace
- Tipos de recursos definidos por el servicio de compilación de imágenes de AWS Marketplace
- Claves de condición para el servicio de compilación de imágenes de AWS Marketplace

Acciones definidas por el servicio de compilación de imágenes de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBuilds [solo permiso]	Describe las compilaciones de imágenes identificadas por un ID de compilación	Read			
ListBuilds [solo permiso]	Muestra las compilaciones de imágenes.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartBuild [solo permiso]	Inicia una compilación de imágenes	Write			

Tipos de recursos definidos por el servicio de compilación de imágenes de AWS Marketplace

AWS Marketplace Image Building Service no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al servicio de compilación de imágenes de AWS Marketplace , especifique `"Resource": "*"` en su política.

Claves de condición para el servicio de compilación de imágenes de AWS Marketplace

La compilación de imágenes de Marketplace no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Marketplace Management Portal

AWS Marketplace El portal de administración (prefijo de servicio:`aws-marketplace-management`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace Management Portal
- Tipos de recursos definidos por AWS Marketplace Management Portal
- Claves de condición para AWS Marketplace Management Portal

Acciones definidas por AWS Marketplace Management Portal

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAdditionalSellerNotificationRecipients [solo permiso]	Concede permiso para ver destinatarios de notificaciones al vendedor adicionales	Lectura			
GetBankAccountVerificationDetails [solo permiso]	Concede permiso para ver el estado de la verificación de la cuenta bancaria	Lectura			
GetSecondaryUserVerificationDetails [solo permiso]	Concede permiso para ver el estado de la verificación de la cuenta de usuario secundaria	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSellerVerificationDetails [solo permiso]	Concede permiso para ver el estado de la verificación de la cuenta	Lectura			
PutAdditionalSellerNotificationRecipients [solo permiso]	Concede permiso para actualizar destinatarios de notificaciones al vendedor adicionales	Escritura			
PutBankAccountVerificationDetails [solo permiso]	Concede permiso para actualizar el estado de la verificación de la cuenta bancaria	Escritura			
PutSecondaryUserVerificationDetails [solo permiso]	Concede permiso para actualizar el estado de la verificación de la cuenta de usuario secundaria	Escritura			
PutSellerVerificationDetails [solo permiso]	Concede permiso para actualizar el estado de la verificación de la cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
uploadFiles [solo permiso]	Permite acceder a la página de carga de archivos dentro del portal AWS Marketplace de administración	Escritura			
viewMarketing [solo permiso]	Permite el acceso a la página de marketing del portal AWS Marketplace de administración	Enumeración			
viewReports [solo permiso]	Permite el acceso a la página de informes del portal AWS Marketplace de administración	Enumeración			
viewSettings [solo permiso]	Permite el acceso a la página de configuración del portal AWS Marketplace de administración	Enumeración			
viewSupport [solo permiso]	Permite el acceso a la página de elegibilidad de Customer Support dentro del Portal AWS Marketplace de Administración	Enumeración			

Tipos de recursos definidos por AWS Marketplace Management Portal

AWS Marketplace El portal de administración no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Marketplace Management Portal, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Marketplace Management Portal

Marketplace Portal no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para el servicio de medición de AWS Marketplace

AWS Marketplace Metering Service (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de medición de AWS Marketplace
- Tipos de recursos definidos por el servicio de medición de AWS Marketplace
- Claves de condición para el servicio de medición de AWS Marketplace

Acciones definidas por el servicio de medición de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchMeterUsage	Otorga permiso para publicar registros de medición para un conjunto de clientes de aplicaciones SaaS	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
MeterUsage	Otorga permiso para emitir registros de medición	Escritura			
RegisterUsage	Otorga permiso para comprobar que el cliente que utiliza su software de pago está suscrito a su producto el mismo día AWS Marketplace, lo que le permite protegerse contra el uso no autorizado. Mide el uso de software por tarea de ECS, por hora, prorrateado al segundo.	Escritura			
ResolveCustomer	Otorga permiso para resolver un token de registro CustomerIdentifier y obtener un código de producto	Escritura			

Tipos de recursos definidos por el servicio de medición de AWS Marketplace

AWS Marketplace Metering Service no admite la especificación de un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso al servicio de medición de AWS Marketplace , especifique `"Resource": "*"` en su política.

Claves de condición para el servicio de medición de AWS Marketplace

La medición de Marketplace no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Marketplace Private Marketplace

AWS Marketplace Private Marketplace (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace Private Marketplace
- Tipos de recursos definidos por AWS Marketplace Private Marketplace
- Claves de condición para AWS Marketplace Private Marketplace

Acciones definidas por AWS Marketplace Private Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateProductsWithPrivateMarketplace [solo permiso]	Concede permiso para aprobar una solicitud para que un producto se asocie con Private Marketplace. Esta acción la puede realizar cualquier cuenta de una AWS organización, siempre que el usuario tenga permisos para hacerlo y las políticas	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de control de servicios de la organización lo permitan				
CreatePrivateMarketplaceRequests [solo permiso]	Concede permiso para crear una nueva solicitud para que un producto o productos se asocien con Private Marketplace. Esta acción la puede realizar cualquier cuenta de una organización o de una AWS organización, siempre que el usuario tenga permisos para hacerlo y las políticas de control de servicios de la organización lo permitan	Escritura			
DescribePrivateMarketplaceRequests [solo permiso]	Concede permiso para describir las solicitudes y los productos asociados con Private Marketplace. Esta acción la puede realizar cualquier cuenta de una AWS organización, siempre que el usuario tenga permisos para hacerlo y las políticas de control de servicios de la organización lo permitan	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateProductsFromPrivateMarketplace [solo permiso]	Concede permiso para rechazar una solicitud para que un producto se asocie con Private Marketplace. Esta acción la puede realizar cualquier cuenta de una AWS organización, siempre que el usuario tenga permisos para hacerlo y las políticas de control de servicios de la organización lo permitan	Escritura			
ListPrivateMarketplaceRequests [solo permiso]	Concede permiso para obtener una lista que se puede consultar de solicitudes y productos asociados en Private Marketplace. Esta acción la puede realizar cualquier cuenta de una AWS organización, siempre que el usuario tenga permisos para hacerlo y las políticas de control de servicios de la organización lo permitan	Enumeración			

Tipos de recursos definidos por AWS Marketplace Private Marketplace

AWS Marketplace Private Marketplace no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Marketplace Private Marketplace, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Marketplace Private Marketplace

Marketplace no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para la integración de sistemas de adquisición de AWS Marketplace

AWS Marketplace La integración de sistemas de adquisición (prefijo de servicio:`aws-marketplace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la integración de sistemas de adquisición de AWS Marketplace
- Tipos de recursos definidos por la integración de sistemas de adquisición de AWS Marketplace
- Claves de condición para la integración de sistemas de adquisición de AWS Marketplace

Acciones definidas por la integración de sistemas de adquisición de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeProcuremen	Otorga permiso para describir la configuración de integraci	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
tSystemConfiguration [solo permiso]	ón del Sistema de Adquisiciones (por ejemplo, Coupa) para la cuenta individual o para toda la AWS organización, si existe. Esta acción solo la puede realizar la cuenta maestra si se utiliza una organización AWS				
PutProcurementSystemConfiguration [solo permiso]	Otorga permiso para crear o actualizar la configuración de integración del Sistema de Adquisiciones (por ejemplo, Coupa) para la cuenta individual o para toda la AWS organización, si existe. Esta acción solo la puede realizar la cuenta maestra si se utiliza una organización AWS	Escritura			

Tipos de recursos definidos por la integración de sistemas de adquisición de AWS Marketplace

AWS Marketplace La integración de sistemas de adquisición no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la integración de sistemas de adquisición de AWS Marketplace , especifique `"Resource": "*"` en su política.

Claves de condición para la integración de sistemas de adquisición de AWS Marketplace

La integración del sistema de compras no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para los Informes de AWS Marketplace

AWS Marketplace Los informes (prefijo de servicio:`aws-marketplace`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por los Informes de AWS Marketplace
- Tipos de recursos definidos por los Informes de AWS Marketplace
- Claves de condición de los Informes de AWS Marketplace

Acciones definidas por los Informes de AWS Marketplace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBuyerDashboard	Otorga permiso para ver un panel que muestra los datos de AWS Marketplace compra del comprador	Lectura	Dashboard *		

Tipos de recursos definidos por los Informes de AWS Marketplace

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Dashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Claves de condición de los Informes de AWS Marketplace

Los Informes de Marketplace no tienen claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones para AWS Marketplace Seller Reporting

AWS Marketplace Los informes sobre vendedores (prefijo de servicio:`aws-marketplace`) proporcionan los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace Seller Reporting
- Tipos de recursos definidos por AWS Marketplace Seller Reporting
- Claves de condición para AWS Marketplace Seller Reporting

Acciones definidas por AWS Marketplace Seller Reporting

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSellerDashboard	Otorga permiso para ver el panel de un vendedor	Lectura	SellerDashboard*		

Tipos de recursos definidos por AWS Marketplace Seller Reporting

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
SellerDashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Claves de condición para AWS Marketplace Seller Reporting

Marketplace Seller Reporting no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights (prefijo de servicio:`vendor-insights`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Marketplace Vendor Insights

- Tipos de recursos definidos por AWS Marketplace Vendor Insights
- Claves de condición de AWS Marketplace Vendor Insights

Acciones definidas por AWS Marketplace Vendor Insights

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateSecurityProfile	Otorga permiso para activar el perfil de seguridad	Escritura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
AssociateDataSource	Otorga permiso para asociar el perfil de seguridad a un origen de datos	Escritura	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
CreateDataSource	Otorga permiso para crear un nuevo origen de datos	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSecurityProfile	Otorga permiso para crear un nuevo perfil de seguridad	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
DeactivateSecurityProfile	Otorga permiso para desactivar el perfil de seguridad	Escritura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Concede permiso para eliminar un origen de datos	Escritura	DataSource*		
				aws:ResourceTag/${TagKey}	
DisassociateDataSource	Otorga permiso para desasociar el perfil de seguridad de un origen de datos	Escritura	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDataSource	Otorga permiso para recuperar los detalles de un origen de datos existente	Lectura	DataSource*		
				aws:ResourceTag/${TagKey}	
GetEntitledSecurityProfileSnapshot	Otorga permiso para devolver los detalles de una instantánea de perfil de seguridad que el solicitante tiene derecho a leer	Lectura	SecurityProfile*		
GetProfileAccessTerms	Otorga permiso para obtener las condiciones de acceso a un perfil de Vendor Insights	Lectura			
GetSecurityProfile	Otorga permiso para devolver los detalles de un perfil de seguridad existente	Lectura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
GetSecurityProfileSnapshot	Otorga permiso para devolver los detalles de una instantánea de perfil de seguridad	Lectura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Otorga permiso para enumerar los orígenes de datos existentes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEntitledSecurityProfileSnapshots	Otorga permiso para devolver la lista de resumen de instantáneas de un perfil de seguridad existente que el solicitante tiene derecho a enumerar	Enumeración	SecurityProfile*		
ListEntitledSecurityProfiles	Otorga permiso para enumerar perfiles de seguridad autorizados	Enumeración			
ListSecurityProfileSnapshots	Otorga permiso para devolver la lista de resumen de instantáneas de un perfil de seguridad existente	Enumeración	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListSecurityProfiles	Otorga permiso para enumerar perfiles de seguridad existentes	Enumeración			
ListTagsForResource	Otorga permiso para enumerar etiquetas para el recurso de información del proveedor	Lectura	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar el recurso de información del proveedor	Etiquetado	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para quitar la etiqueta del recurso de información del proveedor	Etiquetado	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDataSource	Otorga permiso para actualizar un origen de datos existente	Escritura	DataSource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfile	Otorga permiso para actualizar el perfil de seguridad	Escritura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotCreationConfiguration	Otorga permiso para actualizar la configuración de creación de instantáneas del perfil de seguridad	Escritura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotReleaseConfiguration	Otorga permiso para actualizar la configuración del lanzamiento de instantáneas del perfil de seguridad	Escritura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS Marketplace Vendor Insights

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
DataSource	`arn:${Partition}:vendor-insights:::data-source:${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
SecurityProfile	`arn:${Partition}:vendor-insights:::security-profile:${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Claves de condición de AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Mechanical Turk

Amazon Mechanical Turk (prefijo de servicio: `mechanicalturk`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Mechanical Turk
- Tipos de recurso definidos por Amazon Mechanical Turk
- Claves de condición de Amazon Mechanical Turk

Acciones definidas por Amazon Mechanical Turk

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptQualificationRequest	La AcceptQualificationRequest operación concede la solicitud de cualificación de un trabajador	Escritura			
ApproveAssignment	La ApproveAssignment operación aprueba los resultados de una tarea completada	Escritura			
AssociateQualificationWithWorker	La AssociateQualificationWithWorker operación otorga al trabajador una calificación	Escritura			
CreateAdditionalAssignmentsForHIT	La operación CreateAdditionalAssignmentsFor HIT aumenta el número máximo de asignaciones de un HIT existente	Escritura			
CreateHIT	La operación CreateHIT crea una nueva Tarea de inteligencia humana (HIT)	Escritura			
CreateHITType	La HITType operación Crear crea un nuevo tipo de HIT	Escritura			
CreateHITWithHITType	La HITWith HITType operación Create crea una nueva Human Intelligence Task (HIT) utilizando un ID HITType existente generado	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	por la HITType operación Create				
CreateQualificationType	La CreateQualificationType operación crea un nuevo tipo de calificación, que se representa mediante una estructura QualificationType de datos	Escritura			
CreateWorkerBlock	La CreateWorkerBlock operación le permite impedir que un trabajador trabaje en su HITs	Escritura			
DeleteHIT	La operación DeleteHIT elimina una HIT que ya no es necesaria	Escritura			
DeleteQualificationType	Elimina un tipo DeleteQualificationType de calificación y elimina cualquier tipo de HIT que esté asociado con el tipo de calificación	Escritura			
DeleteWorkerBlock	La DeleteWorkerBlock operación le permite reincorporar a un trabajador bloqueado para que trabaje en su HITs	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateQualificationFromWorker	DisassociateQualificationFromWorker Revoca una cualificación previamente otorgada por un usuario	Escritura			
GetAccountBalance	La GetAccountBalance operación recupera la cantidad de dinero de tu cuenta de Amazon Mechanical Turk	Lectura			
GetAssignment	GetAssignment Recupera una tarea con un AssignmentStatus valor de Enviada, Aprobada o Rechazada, utilizando el ID de la tarea	Lectura			
GetFileUploadURL	La operación GetFileUpload URL genera y devuelve una URL temporal	Lectura			
GetHIT	La operación GetHIT recupera los detalles de la HIT especificada	Lectura			
GetQualificationScore	La GetQualificationScore operación devuelve el valor de la cualificación de un trabajador para un tipo de cualificación determinado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQualificationType	La GetQualificationType operación recupera información sobre un tipo de calificación mediante su ID	Lectura			
ListAssignmentsForHIT	La operación ListAssignmentsFor HIT recupera las tareas completadas para un HIT	Enumeración			
ListBonusPayments	La ListBonusPayments operación recupera los importes de las bonificaciones que has pagado a los trabajadores por un HIT o una tarea determinada	Enumeración			
ListHITs	La HITs operación List devuelve todos los datos de un solicitante HITs	Enumeración			
ListHITsForQualificationType	La HITs ForQualificationType operación List devuelve lo HITs que usa lo dado QualififcationType para un QualificationRequirement	Enumeración			
ListQualificationRequests	La ListQualificationRequests operación recupera las solicitudes de cualificaciones de un tipo de cualificación concreto	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQualificationTypes	La ListQualificationTypes operación busca los tipos de cualificación mediante la consulta de búsqueda especificada y devuelve una lista de los tipos de cualificación	Enumeración			
ListReviewPolicyResultsForHIT	La operación ListReviewPolicyResultsFor HIT recupera los resultados calculados y las acciones realizadas durante la ejecución de sus políticas de revisión durante una operación CreateHit.	Enumeración			
ListReviewableHITs	La ListReviewable HITs operación devuelve todos los datos del solicitante HITs que no han sido aprobados o rechazados	Enumeración			
ListWorkerBlocks	La ListWorkersBlocks operación recupera una lista de los trabajadores a los que se les ha impedido trabajar en su HITs	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorkersWithQualificationType	La ListWorkersWithQualificationType operación devuelve todos los trabajadores con un tipo de cualificación determinado	Enumeración			
NotifyWorkers	La NotifyWorkers operación envía un correo electrónico a uno o más trabajadores que usted especifique con el ID de trabajador	Escritura			
RejectAssignment	La RejectAssignment operación rechaza los resultados de una tarea completada	Escritura			
RejectQualificationRequest	La RejectQualificationRequest operación rechaza la solicitud de cualificación de un usuario	Escritura			
SendBonus	La SendBonus operación emite un pago de dinero desde su cuenta a un trabajador	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendTestEventNotification	La SendTestEventNotification operación hace que Amazon Mechanical Turk envíe un mensaje de notificación como si se hubiera producido un evento HIT, de acuerdo con la especificación de notificación proporcionada	Escritura			
UpdateExpirationForHIT	La operación UpdateExpirationFor HIT le permite extender el tiempo de caducidad de una visita más allá de su fecha de caducidad actual o hacer caducar una visita inmediatamente	Escritura			
UpdateHITReviewStatus	La operación de actualización HITReview del estado cambia el estado de un HIT	Escritura			
UpdateHITTypeOfHIT	La operación HITType de actualización de un HIT permite cambiar las HITType propiedades de un HIT	Escritura			
UpdateNotificationSettings	La UpdateNotificationSettings operación crea, actualiza, deshabilita o vuelve a habilitar las notificaciones para un tipo HIT	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQualificationType	La UpdateQualificationType operación modifica los atributos de un tipo de calificación existente, que se representa mediante una estructura de datos QualificationType	Escritura			

Tipos de recurso definidos por Amazon Mechanical Turk

Amazon Mechanical Turk no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Amazon Mechanical Turk, especifique `"Resource": "*"` en su política.

Claves de condición de Amazon Mechanical Turk

MechanicalTurk no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon MemoryDB

Amazon MemoryDB (prefijo de servicio: `memorydb`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para usarse en las políticas de permisos del IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon MemoryDB
- Tipos de recursos definidos por Amazon MemoryDB
- Claves de condición de Amazon MemoryDB

Acciones definidas por Amazon MemoryDB

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Al crear una política de MemoryDB for Redis en IAM debe utilizar el carácter comodín "*" para el bloque de recursos. Para obtener más información acerca del uso de las siguientes acciones de API de MemoryDB for Redis en una política de IAM, consulte Acciones de MemoryDB e IAM.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchUpdateCluster	Otorga permisos para aplicar actualizaciones en un servicio	Escritura	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
				aws:ResourceTag/${TagKey}	
Connect	Permite a un usuario o rol de IAM conectarse como un usuario de MemoryDB especificado a un nodo de un clúster	Escritura	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	
CopySnapshot	Otorga permisos para realizar una copia de una instantánea existente	Escritura	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	Otorga permisos para crear una nueva lista de control de acceso	Escritura	user*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCluster	Otorga permisos para crear un clúster	Escritura	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateMultiRegionCluster	Otorga permisos para crear un clúster multirregional	Escritura	multiregionparametergroup*		memorydb:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateParameterGroup	Otorga permisos para crear un nuevo grupo de parámetros	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateSnapshot	Otorga permisos para crear una copia de seguridad de un clúster en el momento actual	Escritura	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubnetGroup	Otorga permisos para crear un nuevo grupo de subred	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateUser	Otorga permisos para crear un nuevo usuario	Escritura		aws:RequestTag/${TagKey} aws:TagKeys memorydb:UserAuthenticationMode	memorydb:TagResource
DeleteAcl	Otorga permisos para eliminar una lista de control de acceso	Escritura	acl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeleteCluster	Otorga permisos para eliminar un clúster aprovisionado anteriormente	Escritura	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMultiRegionCluster	Otorga permisos para eliminar un clúster multirregional	Escritura	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	Otorga permisos para eliminar un grupo de parámetros	Escritura	parametergroup*		
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	Otorga permisos para eliminar una instantánea	Escritura	snapshot*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSubnetGroup	Otorga permisos para eliminar un grupo de subredes	Escritura	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteUser	Otorga permisos para eliminar un usuario	Escritura	user*		
				aws:ResourceTag/${TagKey}	
DescribeAcls	Otorga permisos para recuperar información sobre las listas de control de acceso	Lectura	acl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DescribeClusters	Otorga permisos para recuperar información sobre todos los clústeres aprovisionados, si no se especifica ningún identificador de clúster, o sobre un clúster específico si se suministra un identificador de clúster	Lectura	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	Otorga permisos para enumerar los motores disponibles y sus versiones	Lectura			
DescribeEvents	Otorga permisos para recuperar eventos relacionados con clústeres, grupos de seguridad de subredes y grupos de parámetros	Lectura			
DescribeMultiRegionClusters	Otorga permisos para recuperar información sobre todos los clústeres multirregionales si no se especifica un identificador de clúster, o sobre un clúster multirregional específico si se proporciona un identificador de clúster	Lectura	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMultiRegionParameterGroups	Otorga permisos para recuperar información sobre los grupos de parámetros multirregionales	Lectura	multiregionparametergroup*		
DescribeMultiRegionParameters	Otorga permisos para recuperar una lista de parámetros detallada para un grupo de parámetros multirregional concreto	Lectura	multiregionparametergroup*		
DescribeParameterGroups	Otorga permisos para recuperar información sobre grupos de parámetros	Lectura	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeParameters	Otorga permisos para recuperar la lista de parámetros detallada de un grupo de parámetros determinado	Lectura	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	Concede permiso para recuperar los nodos reservados	Lectura	reservednode*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReservedNodesOfferings	Concede permisos para recuperar las ofertas de los nodos reservados	Lectura			
DescribeServiceUpdates	Otorga permisos para recuperar los detalles de las actualizaciones del servicio	Lectura			
DescribeSnapshots	Otorga permisos para recuperar información sobre instantáneas de clúster	Lectura	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeSubnetGroups	Otorga permisos para recuperar una lista de grupos de subredes	Lectura	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Otorga permisos para recuperar información sobre los usuarios	Lectura	user*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
FailoverShard	Otorga permisos para probar la conmutación por error automática en una partición especificada en un clúster	Escritura	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
ListAllowedMultiRegionClusterUpdates	Otorga permisos para enumerar las actualizaciones de clústeres multirregionales disponibles	Lectura	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAllowedNodeTypeUpdates	Otorga permisos para enumerar las actualizaciones de tipos de nodo disponibles	Lectura	cluster*		
				aws:ResourceTag/${TagKey}	
ListTags	Otorga permisos para enumerar todas las etiquetas para la asignación de costos	Lectura	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	
PurchaseReservedNodesOffering	Concede permiso para adquirir un nuevo nodo reservado	Escritura	reservednode*		memorydb:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	Otorga permisos para modificar los parámetros de un grupo de parámetros al valor predeterminado del motor o del sistema	Escritura	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	Otorga permisos para agregar hasta 10 etiquetas de asignación de costos al recurso con nombre	Etiquetado	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			reservednode		
			snapshot		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permisos para eliminar de un recurso las etiquetas identificadas en la TagKeys lista	Etiquetado	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	Otorga permisos para actualizar una lista de control de acceso	Escritura	acl*		
			user*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	Otorga permisos para actualizar la configuración de un clúster	Escritura	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	
UpdateMultiRegionCluster	Otorga permisos para actualizar la configuración de un clúster multirregional	Escritura	multiregioncluster *		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregionparametergroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateParameterGroup	Otorga permisos para actualizar los parámetros de un grupo de parámetros	Escritura	parametergroup*		
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	Otorga permisos para actualizar un grupo de subredes	Escritura	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	Otorga permisos para actualizar un usuario	Escritura	user*		
				aws:ResourceTag/${TagKey} memorydb:UserAuthenticationMode	

Tipos de recursos definidos por Amazon MemoryDB

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
multiregionparametergroup	`arn:${Partition}:memorydb::${Account}:multiregionparametergroup/${MultiRegionParameterGroupName}`	
parametergroup	`arn:${Partition}:memorydb:${Region}:${Account}:parametergroup/${ParameterGroupName}`	aws:ResourceTag/${TagKey}
subnetgroup	`arn:${Partition}:memorydb:${Region}:${Account}:subnetgroup/${SubnetGroupName}`	aws:ResourceTag/${TagKey}
multiregioncluster	`arn:${Partition}:memorydb::${Account}:multiregioncluster/${ClusterName}`	aws:ResourceTag/${TagKey} memorydb:TLSEnabled
cluster	`arn:${Partition}:memorydb:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:memorydb:${Region}:${Account}:snapshot/${SnapshotName}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:memorydb:${Region}:${Account}:user/${UserName}`	aws:ResourceTag/${TagKey}
acl	`arn:${Partition}:memorydb:${Region}:${Account}:acl/${AclName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
reservednode	`arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon MemoryDB

Amazon MemoryDB define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso.	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se pasan en la solicitud	ArrayOfString
memorydb:TLSEnabled	Filtra el acceso según el TLSEnabled parámetro presente en la solicitud o, si el parámetro no está presente, el valor predeterminado es verdadero	Bool
memorydb:UserAuthenticationMode	Filtra el acceso mediante el parámetro UserAuthenticationMode .Type de la solicitud	Cadena

Acciones, recursos y claves de condición para el Servicio de entrega de mensajes de Amazon

El Servicio de entrega de mensajes de Amazon (prefijo de servicio: `ec2messages`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio de entrega de mensajes de Amazon
- Tipos de recurso definidos por el Servicio de entrega de mensajes de Amazon
- Claves de condición para el Servicio de entrega de mensajes de Amazon

Acciones definidas por el servicio de entrega de mensajes de Amazon

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcknowledgeMessage	Otorga permiso para confirmar un mensaje, lo que garantiza que no se volverá a entregar.	Write			
DeleteMessage	Otorga permiso para eliminar un mensaje.	Write			
FailMessage	Otorga permiso para suspender un mensaje, lo	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	que indica que el mensaje no se pudo procesar correctamente y garantiza que no pueda responderse ni entregarse de nuevo.				
GetEndpoint	Otorga permiso para dirigir el tráfico al punto de enlace correcto en función del destino de los mensajes.	Lectura			
GetMessages	Otorga permiso para entregar mensajes a clients/instances través de sondeos prolongados	Lectura		ssm:SourceInstanceARN ec2:SourceInstanceARN	
SendReply	Otorga permiso para enviar respuestas desde clients/instances un servicio anterior	Escritura		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Tipos de recurso definidos por el Servicio de entrega de mensajes de Amazon

El servicio de entrega de mensajes de Amazon no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso al servicio de entrega de mensajes de Amazon, especifique `"Resource": "*"` en su política.

Claves de condición para el Servicio de entrega de mensajes de Amazon

Amazon Message Delivery Service define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
ec2:SourceInstanceARN	Filtra acceso por ARN de la instancia en la que se originó la solicitud	ARN
ssm:SourceInstanceARN	Filtra el acceso verificando el nombre de recurso de Amazon (ARN) de AWS la instancia gestionada por el administrador de sistemas desde la que se realiza la solicitud. Esta clave no está presente cuando la solicitud proviene de la instancia gestionada autenticada con un rol de IAM asociado al perfil de la instancia EC2	ARN

Acciones, recursos y claves de condición para el Servicio de puerta de enlace de mensajes de Amazon

El Servicio de puerta de enlace de mensajes de Amazon (prefijo del servicio: `ssmmessages`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el Servicio de puerta de enlace de mensajes de Amazon
- Tipos de recursos definidos por el Servicio de puerta de enlace de mensajes de Amazon
- Claves de condición para el Servicio de puerta de enlace de mensajes de Amazon

Acciones definidas por el Servicio de puerta de enlace de mensajes de Amazon

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateControlChannel	Otorga permiso para registrar un canal de control para que una instancia envíe mensajes de control al servicio Systems Manager.	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	
CreateDataChannel	Otorga permiso para registrar un canal de datos para que una instancia envíe mensajes de datos al servicio Systems Manager.	Write			
OpenControlChannel	Otorga permiso para abrir una conexión websocket para una transmisión de canal del control registrado desde una instancia al servicio Systems Manager.	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
OpenDataChannel	Otorga permiso para abrir una conexión websocket para una transmisión de canal de datos registrado desde una instancia al servicio Systems Manager.	Escritura			

Tipos de recursos definidos por el Servicio de puerta de enlace de mensajes de Amazon

El Servicio de puerta de enlace de mensajes de Amazon no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir acceso al Servicio de puerta de enlace de mensajes de Amazon, especifique `"Resource": "*"` en la política.

Claves de condición para el Servicio de puerta de enlace de mensajes de Amazon

El Servicio de puerta de enlace de mensajes de Amazon define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
ec2:SourceInstanceARN	Filtra acceso por ARN de la instancia en la que se originó la solicitud	ARN
ssm:SourceInstanceARN	Filtra el acceso verificando el nombre de recurso de Amazon (ARN) de AWS la instancia gestionada por el	ARN

Claves de condición	Descripción	Tipo
	administrador de sistemas desde la que se realiza la solicitud. Esta clave no está presente cuando la solicitud proviene de la instancia gestionada autenticada con un rol de IAM asociado al perfil de la instancia EC2	

Acciones, recursos y claves de condición para AWS Microservice Extractor for .NET

AWS Microservice Extractor para .NET (prefijo de servicio:`serviceextract`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Microservice Extractor for .NET
- Tipos de recurso definidos por AWS Microservice Extractor for .NET
- Claves de condición para AWS Microservice Extractor for .NET

Acciones definidas por AWS Microservice Extractor for .NET

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConfig [solo permiso]	Otorga permiso para obtener la configuración necesaria para el cliente de AWS escritorio Microservice Extractor para .NET	Lectura			

Tipos de recurso definidos por AWS Microservice Extractor for .NET

AWS Microservice Extractor para .NET no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Microservice Extractor for .NET, especifique el `"Resource": "*"` en su política.

Claves de condición para AWS Microservice Extractor for .NET

Microservice Extractor for .NET no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para los Créditos del programa de aceleración de la migración de AWS

AWS Migration Acceleration Program Credits (prefijo de servicio:`mapcredits`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones que definen los Créditos del programa de aceleración de la migración de AWS
- Tipos de recursos que definen los Créditos del programa de aceleración de la migración AWS
- Claves de condición para los Créditos del programa de aceleración de la migración AWS

Acciones que definen los Créditos del programa de aceleración de la migración de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssociatedPrograms [solo permiso]	Otorga permiso para ver los acuerdos del Programa de aceleración de la migración que se encuentran asociados al usuario	Enumeración	agreement*		
ListQuarterCredits [solo permiso]	Otorga permiso para ver los acuerdos del Programa de aceleración de la migración y los créditos que se encuentran asociados a la cuenta de pago del usuario	Enumeración	agreement*		
ListQuarterSpend [solo permiso]	Otorga permiso para ver los acuerdos del Programa de aceleración de la migración y los gastos elegibles que se encuentran asociados a la cuenta de pago del usuario	Enumeración	agreement*		

Tipos de recursos que definen los Créditos del programa de aceleración de la migración AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
agreement	`arn:${Partition}:mapcredits:::${Agreement}/${AgreementId}`	

Claves de condición para los Créditos del programa de aceleración de la migración AWS

MapCredits no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Migration Hub

AWS Migration Hub (prefijo de servicio:`mgh`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Migration Hub
- Tipos de recursos definidos por AWS Migration Hub
- Claves de condición para AWS Migration Hub

Acciones definidas por AWS Migration Hub

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptConnection	Otorga permiso para aceptar una conexión	Escritura	ConnectionResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
AssociateAutomationUnitRole	Otorga permiso para asociar un rol de IAM a una unidad de automatización	Escritura	AutomationUnitResource*		
AssociateCreatedArtifact	Otorga permiso para asociar un AWS artefacto determinado a un MigrationTask	Escritura	migrationTask*		
AssociateDiscoveredResource	Otorga permiso para asociar un recurso ADS determinado a un MigrationTask	Escritura	migrationTask*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateSourceResource	Otorga permiso para asociar un recurso fuente	Escritura	migrationTask*		
BatchAssociateIamRoleWithConnection	Otorga permiso para asociar por lotes funciones de IAM a una conexión	Escritura	ConnectionResource*		
BatchDisassociateIamRoleFromConnection	Otorga permiso para desasociar por lotes las funciones de IAM de una conexión	Escritura	ConnectionResource*		
CreateAutomationRun	Otorga permiso para crear una ejecución de unidades de automatización	Escritura			
CreateAutomationUnit	Otorga permiso para crear una unidad de automatización	Escritura			
CreateHomeRegionControl	Concede permiso para crear un control de región inicial de un Migration Hub	Escritura			
CreateProgressUpdateStream	Otorga permiso para crear un ProgressUpdateStream	Escritura	progressUpdateStream*		
DeleteAutomationRun	Otorga permiso para eliminar la ejecución de una unidad de automatización	Escritura	AutomationRunResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAutomationUnit	Otorga permiso para eliminar una unidad de automatización	Escritura	AutomationUnitResource*		
DeleteConnection	Concede permiso para eliminar una conexión.	Escritura	ConnectionResource*		
DeleteHomeRegionControl	Concede permiso para eliminar un control de región inicial de un Migration Hub	Escritura			
DeleteProgressUpdateStream	Otorga permiso para eliminar un ProgressUpdateStream	Escritura	progressUpdateStream*		
DescribeApplicationState	Concede permiso para obtener un estado de la aplicación Application Discovery Service.	Lectura			
DescribeAutomationRun	Otorga permiso para describir el funcionamiento de una unidad de automatización	Lectura	AutomationRunResource*		
DescribeAutomationUnit	Otorga permiso para describir una unidad de automatización	Lectura	AutomationUnitResource*		
DescribeHomeRegionControls	Concede permiso para enumerar controles de región inicial	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMigrationTask	Otorga permiso para describir un MigrationTask	Lectura	migrationTask*		
DisassociateAutomationUnitRole	Otorga permiso para desasociar un rol de IAM de una unidad de automatización	Escritura	AutomationUnitResource*		
DisassociateCreatedArtifact	Otorga permiso para desasociar un artefacto determinado AWS de un MigrationTask	Escritura	migrationTask*		
DisassociateDiscoveredResource	Otorga permiso para desasociar un recurso de ADS determinado de un Migration Task	Escritura	migrationTask*		
DisassociateSourceResource	Otorga permiso para diasociar un recurso fuente	Escritura	migrationTask*		
GetConnection	Concede permiso para obtener una conexión	Lectura	ConnectionResource*		
GetHomeRegion	Concede permiso para obtener la región de inicio de un Migration Hub	Lectura			
ImportMigrationTask	Otorga permiso para importar un MigrationTask	Escritura	migrationTask*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApplicationStates	Concede permiso para enumerar estados de aplicaciones	Enumeración			
ListAutomationRuns	Otorga permiso para enumerar las ejecuciones de las unidades de automatización	Enumeración			
ListAutomationUnits	Otorga permiso para enumerar las unidades de automatización	Enumeración			
ListConnectionRoles	Otorga permiso para enumerar las funciones de conexión	Enumeración	ConnectionResource*		
ListConnections	Otorga permiso para enumerar las conexiones	Enumeración			
ListCreatedArtifacts	Otorga permiso para enumerar los artefactos creados asociados a un MigrationTask	Enumeración	migrationTask*		
ListDiscoveredResources	Otorga permiso para enumerar los recursos de ADS asociados de MigrationTask	Enumeración	migrationTask*		
ListMigrationTaskUpdates	Otorga permiso para enumerar las actualizaciones de las tareas de migración	Enumeración	migrationTask*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMigrationTasks	Otorga permiso para publicar MigrationTasks	Enumeración			
ListProgressUpdateStreams	Otorga permiso para publicar ProgressUpdateStreams	Enumeración			
ListSourceResources	Otorga permiso para enumerar los recursos fuente	Enumeración	migrationTask*		
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	Enumeración			
NotifyApplicationState	Concede permiso para actualizar un estado de la aplicación Application Discovery Service.	Escritura			
NotifyMigrationTaskState	Otorga permiso para notificar al MigrationTask estado más reciente	Escritura	migrationTask*		
PutResourceAttributes	Otorga permiso para poner ResourceAttributes	Escritura	migrationTask*		
RejectConnection	Otorga permiso para rechazar una conexión	Escritura	ConnectionResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar un recurso	Etiquetado		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado		aws:TagKeys	

Tipos de recursos definidos por AWS Migration Hub

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
progressUpdateStream	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}`	
migrationTask	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}`	

Tipos de recurso	ARN	Claves de condición
AutomationRunResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-run/${RunID}`	mgh:AutomationRunResourceRunID
AutomationUnitResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-unit/${AutomationUnitId}`	mgh:AutomationUnitResourceAutomationUnitArn
ConnectionResource	`arn:${Partition}:mgh:${Region}:${Account}:${ConnectionArn}`	aws:ResourceTag/${TagKey} mgh:ConnectionResourceConnectionArn

Claves de condición para AWS Migration Hub

AWS Migration Hub define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString
mgh:AutomationRunResourceRunID	AutomationRunResource identificador RunID del recurso	Cadena
mgh:AutomationUnitResourceAutomationUnitArn	AutomationUnitResource identificador de recursos automationUnitArn	ARN
mgh:ConnectionResourceConnectionArn	ConnectionResource identificador de conexión de recursos (ARN)	Cadena

Acciones, recursos y claves de condición para AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator (prefijo de servicio:`migrationhub-orchestrator`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Migration Hub Orchestrator
- Tipos de recursos definidos por AWS Migration Hub Orchestrator
- Claves de condición para AWS Migration Hub Orchestrator

Acciones definidas por AWS Migration Hub Orchestrator

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTemplate	Concede permiso para crear una plantilla personalizada	Escritura			
CreateWorkflow	Otorga permiso para crear un flujo de trabajo basado en la plantilla seleccionada	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowStep	Otorga permiso para crear un paso en un flujo de trabajo y un grupo de pasos específico	Escritura	workflow*		
CreateWorkflowStepGroup	Otorga permiso para crear un grupo de pasos personalizado para un flujo de trabajo determinado	Escritura	workflow*		
DeleteTemplate	Concede permiso para eliminar una plantilla personalizada	Escritura	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteWorkflow	Otorga permiso para crear un flujo de trabajo	Escritura	workflow*		
DeleteWorkflowStep	Otorga permiso para eliminar un paso de un grupo de pasos específico en un flujo de trabajo	Escritura	workflow*		
DeleteWorkflowStepGroup	Otorga permiso para eliminar un grupo de pasos asociado a un flujo de trabajo	Escritura	workflow*		
GetMessage	Otorga permiso al complemento para recibir información del servicio	Lectura			
GetTemplate	Otorga permiso para recuperar los metadatos de una plantilla	Lectura	template*		
GetTemplateStep	Otorga permiso para recuperar detalles de un paso asociado a una plantilla y a un grupo de pasos	Lectura	template*		
GetTemplateStepGroup	Otorga permiso para recuperar metadatos de un grupo de pasos en una plantilla	Lectura	template*		
GetWorkflow	Otorga permiso para recuperar metadatos asociados a un flujo de trabajo	Lectura	workflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetWorkflowStep	Otorga permiso para obtener detalles del paso asociado a un flujo de trabajo y un grupo de pasos	Lectura	workflow*		
GetWorkflowStepGroup	Otorga permiso para obtener detalles de un grupo de pasos asociado a un flujo de trabajo	Lectura	workflow*		
ListPlugins	Otorga permiso para obtener una lista de todos los complementos registrados	Enumeración			
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas para el recurso especificado	Lectura	template* workflow*		
ListTemplateStepGroups	Otorga permiso para enumerar los grupos de pasos de una plantilla	Enumeración	template*		
ListTemplateSteps	Otorga permiso para obtener una lista de pasos de un grupo de pasos	Enumeración	template*		
ListTemplates	Otorga permiso para obtener una lista de todas las plantillas disponibles para el cliente	Enumeración			
ListWorkflowStepGroups	Otorga permiso para obtener una lista de los grupos de pasos asociados con un flujo de trabajo	Enumeración	workflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorkflowSteps	Otorga permiso para obtener una lista de pasos dentro del grupo de pasos asociados a un flujo de trabajo	Enumeración	workflow*		
ListWorkflows	Otorga permiso para enumerar todos los flujos de trabajo	Enumeración			
RegisterPlugin	Otorga el permiso para registrar el complemento para recibir un ID y comenzar a recibir mensajes del servicio	Escritura			
RetryWorkflowStep	Otorga permiso para reintentar un paso erróneo dentro de un flujo de trabajo	Escritura	workflow*		
SendMessage	Otorga permiso al complemento para enviar información al servicio	Escritura			
StartWorkflow	Otorga permiso para iniciar un flujo de trabajo o reanudar un flujo de trabajo detenido	Escritura	workflow*		
StopWorkflow	Otorga permiso para detener un flujo de trabajo	Escritura	workflow*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	template workflow		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	template		
			workflow		
				aws:TagKeys	
UpdateTemplate	Concede permiso para actualizar una plantilla personalizada	Escritura	template*		
UpdateWorkflow	Otorga permiso para actualizar metadatos asociados a un flujo de trabajo	Escritura	workflow*		
UpdateWorkflowStep	Otorga permiso para actualizar los metadatos y el estado de un paso personalizado dentro de un flujo de trabajo	Escritura	workflow*		
UpdateWorkflowStepGroup	Otorga permiso para actualizar metadatos asociados a un grupo de pasos en un flujo de trabajo determinado	Escritura	workflow*		

Tipos de recursos definidos por AWS Migration Hub Orchestrator

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
workflow	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:workflow/${ResourceId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces (prefijo de servicio:`refactor-spaces`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Migration Hub Refactor Spaces
- Tipos de recursos definidos por AWS Migration Hub Refactor Spaces
- Claves de condición de AWS Migration Hub Refactor Spaces

Acciones definidas por AWS Migration Hub Refactor Spaces

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Otorga permiso para crear una aplicación dentro de un entorno.	Escritura		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Concede permiso para crear un entorno.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoute	Otorga permiso para crear una ruta dentro de una aplicación.	Escritura		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:Se	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				rviceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateService	Otorga permiso para crear un servicio dentro de una aplicación.	Escritura		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Otorga permiso para eliminar una aplicación de un entorno.	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
DeleteEnvironment	Concede permiso para eliminar un entorno.	Escritura	environment*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos.	Escritura			
DeleteRoute	Otorga permiso para eliminar una ruta de una aplicación	Escritura	route*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	
DeleteService	Otorga permiso para eliminar un servicio de una aplicación.	Escritura	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetApplication	Otorga permiso para obtener más información sobre una aplicación	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetEnvironment	Otorga permiso para obtener más información para un entorno.	Lectura	environment*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Otorga permiso para obtener información detallada sobre una política de recurso.	Lectura			
GetRoute	Otorga permiso para obtener más información sobre una ruta.	Lectura	route*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetService	Otorga permiso para obtener más información sobre un servicio.	Lectura	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
ListApplications	Otorga permiso para enumerar todas las aplicaciones en un entorno.	Lectura	application*		
ListEnvironmentVpcs	Otorga permiso para enumerar todos VPCs los del entorno	Lectura	environment*		
ListEnvironments	Otorga permiso para enumerar todos los entornos.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRoutes	Otorga permiso para enumerar todas las rutas en una aplicación.	Lectura	route*		
ListServices	Otorga permiso para enumerar todos los servicios en un entorno.	Lectura	environment*		
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas de un recurso determinado.	Lectura			
PutResourcePolicy	Otorga permiso para agregar una política de recursos.	Escritura			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	application		
			environment		
			route		
			service		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	application		
			environment		
			route		
			service		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateRoute	Concede permiso para actualizar una ruta de una aplicación	Escritura	route*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS Migration Hub Refactor Spaces

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds
service	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/service/${ServiceId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:ServiceCreatedByAccount

Tipos de recurso	ARN	Claves de condición
route	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/route/${RouteId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:RouteCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:SourcePath

Claves de condición de AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
refactor-spaces:ApplicationCreatedByAccount	Filtra el acceso mediante la restricción de la acción solo a las cuentas que crearon la aplicación dentro de un entorno.	Cadena
refactor-spaces:CreatedByAccountIds	Filtra el acceso mediante las cuentas que crearon el recurso.	ArrayOfString
refactor-spaces:RouteCreatedByAccount	Filtra el acceso mediante la restricción de la acción solo a las cuentas que crearon la ruta dentro de una aplicación.	Cadena
refactor-spaces:ServiceCreatedByAccount	Filtra el acceso mediante la restricción de la acción solo a las cuentas que crearon el servicio dentro de una aplicación.	Cadena
refactor-spaces:SourcePath	Filtra el acceso mediante la trayectoria de la ruta.	Cadena

Acciones, recursos y claves de condición para AWS Migration Hub Strategy Recommendations

AWS Las recomendaciones estratégicas de Migration Hub (prefijo de servicio:`migrationhub-strategy`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Migration Hub Strategy Recommendations
- Tipos de recurso definidos por AWS Migration Hub Strategy Recommendations
- Claves de condición para AWS Migration Hub Strategy Recommendations

Acciones definidas por AWS Migration Hub Strategy Recommendations

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAntiPattern	Otorga el permiso para obtener detalles de cada antipatrón que el recopilador debe tener en cuenta en el entorno de un cliente	Lectura			
GetApplicationComponentDetails	Otorga el permiso para obtener los detalles de una aplicación	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetApplicationComponentStrategies	Otorga el permiso para obtener una lista de todas las estrategias y herramientas recomendadas para una aplicación que se ejecuta en un servidor	Lectura			
GetAssessment	Otorga el permiso para recuperar el estado de una evaluación en curso	Lectura			
GetImportFileTask	Otorga el permiso para obtener detalles de una tarea de importación específica	Lectura			
GetLatestAssessmentId	Otorga permiso para recuperar el identificador de evaluación más reciente	Lectura			
GetMessage	Permite al recopilador recibir información del servicio	Lectura			
GetPortfolioPreferences	Otorga permiso para recuperar las preferencias de los clientes migration/ Modernization	Lectura			
GetPortfolioSummary	Otorga el permiso para recuperar el resumen general (número de servidores que se van a volver a alojar, etc., así como el número total de antipatrones)	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRecommendationReportDetails	Otorga el permiso para recuperar información detallada sobre un informe de recomendaciones	Lectura			
GetServerDetails	Otorga el permiso para obtener información acerca de un servidor específico	Lectura			
GetServerStrategies	Otorga el permiso para obtener estrategias y herramientas recomendadas para un servidor específico	Lectura			
ListAnalyzableServers	Otorga permiso para obtener una lista de todos los servidores analizables del entorno de un cliente	Enumeración			
ListAntiPatterns	Otorga el permiso para obtener una lista de todos los antipatrones que el recopilador debe buscar en el entorno de un cliente	Enumeración			
ListApplicationComponents	Otorga el permiso para obtener una lista de todas las aplicaciones que se ejecutan en servidores de los servidores del cliente	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCollectors	Otorga el permiso para obtener una lista de todos los recopiladores que el cliente instala	Enumeración			
ListImportFileTask	Otorga el permiso para obtener una lista de todas las importaciones que el cliente realiza	Enumeración			
ListJarArtifacts	Otorga el permiso para obtener una lista de binarios que el recopilador debe evaluar	Enumeración			
ListServers	Otorga el permiso para obtener una lista de todos los servidores del entorno de un cliente	Enumeración			
PutLogData	Concede permiso al recopilador para enviar registros al servicio	Escritura			
PutMetricData	Concede permiso al recopilador para enviar métricas al servicio	Escritura			
PutPortfolioPreferences	Otorga permiso para guardar Migration/Modernization las preferencias del cliente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterCollector	Otorga el permiso para registrar el recopilador para recibir un ID y comenzar a recibir mensajes del servicio	Escritura			
SendMessage	Permite al recopilador enviar información al servicio	Escritura			
StartAssessment	Otorga el permiso para comenzar la evaluación en el entorno de un cliente (recopilar datos de todos los servidores y proporcionar recomendaciones)	Escritura			
StartImportFileTask	Otorga el permiso para comenzar a importar datos desde un archivo proporcionado por el cliente	Escritura			
StartRecommendationReportGeneration	Otorga el permiso para comenzar a generar un informe de recomendaciones	Escritura			
StopAssessment	Otorga el permiso para detener una evaluación en curso	Escritura			
UpdateApplicationComponentConfig	Otorga el permiso para actualizar los detalles de una aplicación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCollectorConfiguration	Otorga permiso para que el recopilador pueda enviar información de configuración al servicio	Escritura			
UpdateServerConfig	Otorga el permiso para actualizar la información de un servidor junto con la estrategia recomendada	Escritura			

Tipos de recurso definidos por AWS Migration Hub Strategy Recommendations

AWS Las recomendaciones de estrategia de Migration Hub no admiten la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Migration Hub Strategy Recommendations, especifique `"Resource": "*"` en la política.

Claves de condición para AWS Migration Hub Strategy Recommendations

Migration Hub Strategy Recommendations no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Mobile Analytics

Amazon Mobile Analytics (prefijo de servicio: `mobileanalytics`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Mobile Analytics
- Tipos de recurso definidos por Amazon Mobile Analytics
- Claves de condición de Amazon Mobile Analytics

Acciones definidas por Amazon Mobile Analytics

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFinancialReports	Conceden acceso a las métricas financieras de una aplicación.	Read			
GetReports	Conceder acceso a las métricas estándares de una aplicación.	Lectura			
PutEvents	La PutEvents operación registra uno o más eventos	Escritura			

Tipos de recurso definidos por Amazon Mobile Analytics

Amazon Mobile Analytics no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Amazon Mobile Analytics, especifique `"Resource": "*"` en su política.

Claves de condición de Amazon Mobile Analytics

Mobile Analytics no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de instrucciones de política. Para ver la lista de las claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Monitron

Amazon Monitron (prefijo de servicio: `monitron`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Monitron
- Tipos de recursos definidos por Amazon Monitron
- Claves de condición de Amazon Monitron

Acciones definidas por Amazon Monitron

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateProjectAdminUser [solo permiso]	Concede permiso para asociar a un usuario al proyecto como administrador	Permissions management	project*		sso-directory:DescribeUsers sso:AssociateProfile

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProject [solo permiso]	Concede permiso para crear un proyecto.	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole kms:CreateGrant sso:CreateManagedApplicationInstance sso:DeleteManagedApplicationInstance sso:DescribeRegisteredRegions

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProjectUserAssociation [solo permiso]	Concede permiso para asociar a un usuario con el proyecto	Administración de permisos	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateUserAccessRoleAssociation [solo permiso]	Concede permiso para asociar un rol de acceso con el usuario	Administración de permisos	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
DeleteProject [solo permiso]	Concede permiso para eliminar un proyecto.	Write	project*		sso:DeleteManagedApplicationInstance

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteProjectUserAssociation [solo permiso]	Concede permiso para disociar un usuario del proyecto	Administración de permisos	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
DeleteUserAccessRoleAssociation [solo permiso]	Concede permiso para disociar un rol de acceso del usuario	Administración de permisos	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateProjectAdminUser [solo permiso]	Concede permiso para disociar a un administrador del proyecto	Permissions management	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
GetProject [solo permiso]	Concede permiso para obtener información sobre un proyecto	Read	project*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetProjectAdminUser [solo permiso]	Concede permiso para describir a un administrador que está asociado al proyecto	Read	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:ListProfileAssociations
ListProjectAdminUsers [solo permiso]	Concede permiso para enumerar todos los administradores asociados al proyecto	Permissions management	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProjectUserAssociations [solo permiso]	Concede permiso para enumerar todos los usuarios asociados con el proyecto	Enumeración	project*		sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
ListProjects [solo permiso]	Concede permiso para enumerar todos los proyectos	List			
ListTagsForResource [solo permiso]	Concede permiso para obtener una lista de etiquetas para un recurso	Read	project		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListUserAccessRoleAssociations [solo permiso]	Concede permiso para enumerar todos los roles de acceso asociados con el usuario	Enumeración	project*		
TagResource [solo permiso]	Concede permiso para etiquetar un recurso	Etiquetado	project		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [solo permiso]	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	project		
				aws:TagKeys	
UpdateProject [solo permiso]	Concede permiso para actualizar un proyecto	Write	project*		

Tipos de recursos definidos por Amazon Monitron

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
project	`arn:${Partition}:monitron:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Monitron

Amazon Monitron define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas a un recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon MQ

Amazon MQ (prefijo de servicio: `mq`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon MQ
- Tipos de recurso definidos por Amazon MQ
- Claves de condición de Amazon MQ

Acciones definidas por Amazon MQ

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBroker	Otorga permiso para crear un agente.	Write		aws:RequestTag/${TagKey}	ec2:CreateNetworkInterface
				aws:TagKeys	ec2:CreateNetworkInterfacePermission
					ec2:CreateSecurityGroup
					ec2:CreateVpcEndpoint
					ec2:DescribeIntern

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					etGateways ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:CreateServiceLinkedRole route53:AssociateVPCWithHostedZone
CreateConfiguration	Otorga permiso para crear una nueva configuración para el nombre de configuración especificado. Amazon MQ utiliza la configuración predeterminada (el tipo de motor y la versión del motor).	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicaBroker [solo permiso]	Concede permiso para crear un agente de réplicas	Escritura	brokers*		
CreateTags	Otorga permiso para crear etiquetas.	Etiquetado	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateUser	Otorga permiso para crear un usuario de ActiveMQ.	Write	brokers*		
DeleteBroker	Otorga permiso para eliminar un agente.	Escritura	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteConfiguration	Otorga permiso para eliminar una configuración	Escritura	configurations*		
DeleteTags	Otorga permiso para eliminar etiquetas.	Etiquetado	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	Otorga permiso para eliminar un usuario de ActiveMQ.	Write	brokers*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeBroker	Otorga permiso para devolver información acerca del agente especificado.	Read	brokers*		
DescribeBrokerEngineTypes	Otorga permiso para devolver información acerca de los motores del agente.	Read			
DescribeBrokerInstanceOptions	Otorga permiso para devolver información acerca de las opciones de instancia del agente.	Read			
DescribeConfiguration	Otorga permiso para devolver información acerca de la configuración especificada.	Read	configurations*		
DescribeConfigurationRevision	Otorga permiso para devolver la revisión de configuración especificada para la configuración especificada.	Read	configurations*		
DescribeUser	Otorga permiso para devolver información acerca de un usuario de ActiveMQ.	Read	brokers*		
ListBrokers	Otorga permiso para devolver una lista de todos los agentes.	List			
ListConfigurationRevisions	Otorga permiso para devolver una lista de todas las revisiones existentes para la configuración especificada.	List	configurations*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConfigurations	Otorga permiso para devolver una lista de todas las configuraciones.	List			
ListTags	Otorga permiso para devolver una lista de etiquetas	List	brokers		
			configurations		
ListUsers	Otorga permiso para devolver una lista de todos los usuarios de ActiveMQ.	Enumeración	brokers*		
Promote	Otorga permiso para promover un corredor	Escritura	brokers*		
RebootBroker	Otorga permiso para reiniciar un agente.	Write	brokers*		
UpdateBroker	Otorga permiso para agregar un cambio de configuración pendiente a un agente.	Write	brokers*		
UpdateConfiguration	Otorga permiso para actualizar la configuración especificada.	Write	configurations*		
UpdateUser	Otorga permiso para actualizar la información para un usuario de ActiveMQ.	Write	brokers*		

Tipos de recurso definidos por Amazon MQ

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}`	aws:ResourceTag/${TagKey}
configurations	`arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon MQ

Amazon MQ define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones para la aprobación por parte de varias partes

La aprobación multipartita (prefijo de servicio:`mpa`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas mediante la aprobación de varias partes
- Tipos de recursos definidos por la aprobación de varias partes
- Claves de condición para la aprobación multipartita

Acciones definidas mediante la aprobación de varias partes

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelSession	Otorga permiso para cancelar una sesión de aprobación	Escritura	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
CreateApprovalTeam	Otorga permiso para crear un equipo de aprobación	Escritura	approval-team*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdentitySource	Otorga permiso para crear una fuente de identidad	Escritura	identity-source*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteIdentitySource	Otorga permiso para eliminar una fuente de identidad	Escritura	identity-source*		
				aws:ResourceTag/${TagKey}	
DeleteInactiveApprovalTeamVersion	Otorga permiso para eliminar un equipo de aprobación inactivo	Escritura	approval-team*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [solo permiso]	Concede permiso para eliminar una política de recursos	Administración de permisos			
GetApprovalTeam	Otorga permiso para recuperar los detalles de un equipo de aprobación	Lectura	approval-team*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetIdentitySource	Otorga permiso para recuperar los detalles de una fuente de identidad	Lectura	identity-source*		
				aws:ResourceTag/${TagKey}	
GetPolicyVersion	Otorga permiso para recuperar los detalles de una política	Lectura			
GetResourcePolicy	Otorga permiso para recuperar los detalles de un recurso específico	Lectura			
GetSession	Otorga permiso para recuperar detalles para una sesión de aprobación	Lectura	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApprovalTeams	Otorga permiso para incluir los equipos de aprobación	Enumeración			
ListIdentitySources	Otorga permiso para enumerar las fuentes de identidad	Enumeración			
ListPolicies	Otorga permiso para enumerar políticas	Enumeración			
ListPolicyVersions	Otorga permiso para enumerar las versiones de las políticas	Enumeración			
ListResourcePolicies	Otorga permiso para enumerar las políticas de un recurso	Enumeración			
ListSessions	Otorga permiso para enumerar las sesiones de aprobación	Enumeración			
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	List			
PutResourcePolicy [solo permiso]	Otorga permiso para crear o actualizar las políticas de un recurso	Administración de permisos			
StartActiveApprovalTeamDeletion	Otorga permiso para iniciar el proceso de eliminación a un equipo de aprobación activo	Escritura	approval-team*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
StartSession [solo permiso]	Otorga permiso para iniciar una sesión de aprobación	Escritura	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
TagResource	Concede permiso para etiquetar un recurso	Etiquetado		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado		aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateApprovalTeam	Otorga permiso para actualizar el equipo de aprobación	Escritura	approval-team*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por la aprobación de varias partes

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
approval-team	`arn:${Partition}:mpa:${Region}:${Account}:approval-team/${Arn}`	aws:ResourceTag/${TagKey}
identity-source	`arn:${Partition}:mpa:${Region}:${Account}:identity-source/${IdentitySourceArn}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
session	`arn:${Partition}:mpa:${Region}:${Account}:session/${SessionArn}`	aws:ResourceTag/${TagKey}

Claves de condición para la aprobación multipartita

La aprobación multipartidista define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
mpa:ProtectedResourceAccount	Filtra el acceso por la cuenta propietaria del recurso que es el objetivo de la operación que requiere aprobación	Cadena
mpa:RequestedOperation	Filtra el acceso mediante una operación solicitada que requiere la aprobación del equipo antes de poder ejecutarse	Cadena

Acciones, recursos y claves de condición de Amazon Neptune

Amazon Neptune (prefijo de servicio: `neptune-db`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Neptune
- Tipos de recurso definidos por Amazon Neptune
- Claves de condición de Amazon Neptune

Acciones definidas por Amazon Neptune

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelLoaderJob	Otorga permiso para cancelar un trabajo de carga	Escritura	database*		
CancelMLDataProcessingJob	Otorga permiso para cancelar un trabajo de procesamiento de datos de ML	Escritura	database*		
CancelMLModelTrainingJob	Otorga permiso para cancelar un trabajo de formación de modelos de ML	Escritura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelMLModelTransformJob	Otorga permiso para cancelar un trabajo de transformación de modelos de ML	Escritura	database*		
CancelQuery	Otorga permiso para cancelar una consulta	Escritura	database*		
CreateMLEndpoint	Otorga permiso para crear un punto de conexión de ML	Escritura	database*		
DeleteDataViaQuery	Otorga permiso para ejecutar y eliminar datos mediante una consulta APIs en la base de datos	Escritura	database*		
				neptune-db:QueryLanguage	
DeleteMLEndpoint	Otorga permiso para eliminar un punto de conexión de ML	Escritura	database*		
DeleteStatistics	Otorga permiso para eliminar todas las estadísticas de la base de datos	Escritura	database*		
GetEngineStatus	Otorga permiso para verificar el estado del motor Neptune	Lectura	database*		
GetGraphSummary	Concede permiso para obtener el resumen de gráficos de la base de datos	Lectura	database*		
GetLoaderJobStatus	Otorga permiso para verificar el estado de un trabajo de carga	Lectura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMLDataProcessingJobStatus	Otorga permiso para verificar el estado de un trabajo de procesamiento de datos de ML	Lectura	database*		
GetMLEndpointStatus	Otorga permiso para verificar el estado de un punto de conexión de ML	Lectura	database*		
GetMLModelTrainingJobStatus	Otorga permiso para verificar el estado de un trabajo de formación de modelos de ML	Lectura	database*		
GetMLModelTransformJobStatus	Otorga permiso para verificar el estado de un trabajo de transformación de modelos de ML	Lectura	database*		
GetQueryStatus	Otorga permiso para verificar el estado de todas las consultas activas	Lectura	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	Otorgae permiso para verificar el estado de las estadísticas de la base de datos	Lectura	database*		
GetStreamRecords	Otorga permiso para buscar registros de transmisión de Neptune	Lectura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				neptune-db:QueryLanguage	
ListLoaderJobs	Otorga permiso para enumerar todos los trabajos de carga	Enumeración	database*		
ListMLDataProcessingJobs	Otorga permiso para enumerar todos los trabajos de procesamiento de datos de ML	Enumeración	database*		
ListMLEndpoints	Otorga permiso para recuperar una lista de todos los puntos de conexión de ML	Enumeración	database*		
ListMLModelTrainingJobs	Otorga permiso para enumerar todos los trabajos de formación de modelos de ML	Enumeración	database*		
ListMLModelTransformJobs	Otorga permiso para enumerar todos los trabajos de formación de modelos de ML	Enumeración	database*		
ManageStatistics	Otorga permiso para administrar las estadísticas de la base de datos	Escritura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ReadDataViaQuery	Otorga permiso para ejecutar la lectura de datos mediante una consulta APIs en la base de datos	Lectura	database*		
				neptune-db:QueryLanguage	
ResetDatabase	Otorga permiso para obtener el token necesario para restablecimiento y restablece la base de datos de Neptune	Escritura	database*		
StartLoaderJob	Otorga permisos para comenzar un trabajo de carga	Escritura	database*		
StartMLDataProcessingJob	Otorga permiso para comenzar un trabajo de procesamiento de datos de ML	Escritura	database*		
StartMLModelTrainingJob	Otorga permiso para comenzar un trabajo de formación de modelos de ML	Escritura	database*		
StartMLModelTransformJob	Otorga permiso para comenzar un trabajo de transformación de modelos de ML	Escritura	database*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
WriteDataViaQuery	Otorga permiso para ejecutar y escribir datos mediante una consulta APIs en la base de datos	Escritura	database*		
				neptune-db:QueryLanguage	
connect	Otorga permiso a todas las acciones de acceso a datos en las versiones del motor anteriores a la 1.2.0.0	Escritura	database*		

Tipos de recurso definidos por Amazon Neptune

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
database	`arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*`	

Claves de condición de Amazon Neptune

Amazon Neptune define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en

las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
neptune-db:QueryLanguage	Filtra el acceso por modelo de gráfico	Cadena

Acciones, recursos y claves de condición para Analítica de Amazon Neptune

La Analítica de Amazon Neptune (prefijo de servicio: `neptune-graph`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la Analítica de Amazon Neptune
- Tipos de recursos definidos por la Analítica de Amazon Neptune
- Claves de condición para la Analítica de Amazon Neptune

Acciones definidas por la Analítica de Amazon Neptune

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Todas las acciones de IAM, excepto ReadDataViaQuery ',' 'yWriteDataViaQuery' ', tienen una operación de API correspondiente DeleteDataViaQuery

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelExportTask	Otorga permiso para cancelar una tarea de exportación en curso	Escritura	export-task*		
				aws:ResourceTag/${TagKey}	
CancelImportTask	Concede permiso para cancelar una tarea de importación en curso	Escritura	import-task*		
CancelQuery	Otorga permiso para cancelar una consulta	Escritura	graph*		
				aws:ResourceTag/${TagKey}	
CreateGraph	Concede permiso para crear un nuevo gráfico	Escritura	graph*		iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
CreateGraphSnapshot	Concede permisos para crear una nueva instantánea a partir de un gráfico existente	Escritura	graph* graph-snapshot*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGraphUsingImportTask	Concede permiso para crear un nuevo gráfico al importar datos al nuevo gráfico	Escritura	graph*		iam:CreateServiceLinkedRole iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey
			import-task*		
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePrivateGraphEndpoint	Concede permiso para crear un nuevo punto de conexión de gráfico privado para acceder al gráfico desde una vpc	Escritura	graph*		ec2:CreateVpcEndpoint ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:AssociateV

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					PCWithHostedZone
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteDataViaQuery	Otorga permiso para eliminar datos mediante una consulta APIs en el gráfico	Escritura	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraph	Concede permiso para eliminar un gráfico	Escritura	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraphSnapshot	Concede permisos para eliminar una instantánea	Escritura	graph-snapshot*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePrivateGraphEndpoint	Concede permiso para eliminar un punto de conexión de gráfico privado de un gráfico	Escritura	graph*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:Disassocia

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					teVPCFromHostedZone
				aws:ResourceTag/${TagKey}	
GetEngineStatus	Concede permiso para obtener el estado del motor del gráfico	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
GetExportTask	Otorga permiso para obtener detalles sobre una tarea de exportación	Lectura	export-task*		
				aws:ResourceTag/${TagKey}	
GetGraph	Concede permiso para obtener detalles sobre un gráfico	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
GetGraphSnapshot	Concede permiso para obtener detalles sobre una instantánea	Lectura	graph-snapshot*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGraphSummary	Concede permiso para obtener el resumen de los datos del gráfico	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
GetImportTask	Concede permiso para obtener los detalles de una tarea de importación	Lectura	import-task*		
GetPrivateGraphEndpoint	Concede permiso para obtener detalles sobre un punto de conexión de gráfico privado de un gráfico	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
GetQueryStatus	Concede permiso para verificar el estado de una consulta determinada	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
GetStatisticsStatus	Concede permiso para obtener las estadísticas de los datos del gráfico	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
ListExportTasks	Otorga permiso para enumerar las tareas de exportación en su cuenta	Lectura	export-task*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGraphSnapshots	Concede permiso para enumerar las instantáneas de su cuenta	Lectura	graph-snapshot*		
ListGraphs	Concede permiso para enumerar los gráficos de su cuenta	Lectura	graph*		
ListImportTasks	Concede permiso para enumerar las tareas de importación de su cuenta	Lectura	import-task*		
ListPrivateGraphEndpoints	Concede permiso para enumerar los puntos de conexión del gráfico privado de un gráfico determinado	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
ListQueries	Otorga permiso para verificar el estado de todas las consultas activas	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permiso a la etiqueta de listas para un recurso de Neptune Analytics	Lectura	graph		
			graph-snapshot		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ReadDataViaQuery	Otorga permiso para leer los datos mediante una consulta APIs en el gráfico	Lectura	graph*		
				aws:ResourceTag/${TagKey}	
ResetGraph	Concede permiso para restablecer un gráfico, lo que elimina todos los datos del gráfico	Escritura	graph*		
				aws:ResourceTag/${TagKey}	
RestoreGraphFromSnapshot	Concede permiso para crear un gráfico a partir de una instantánea existente	Escritura	graph*		kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph-snapshot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
StartExportTask	Otorga permiso para exportar datos de un gráfico existente	Escritura	export-task*		iam:PassRole
			graph*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartImportTask	Concede permiso para importar datos a un gráfico existente	Escritura	graph*		iam:PassRole
			import-task*		
TagResource	Concede permiso para etiquetar un recurso de Neptune Analytics	Etiquetado	graph		
			graph-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para desetiquetar un recurso de Neptune Analytics	Etiquetado	graph		
			graph-snapshot		
				aws:TagKeys	
UpdateGraph	Concede permiso para modificar un gráfico	Escritura	graph*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} neptune-graph:PublicConnectivity	
WriteDataViaQuery	Otorga permiso para escribir datos mediante una consulta APIs en el gráfico	Escritura	graph*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por la Analítica de Amazon Neptune

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
graph	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
graph-snapshot	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}
import-task	`arn:${Partition}:neptune-graph:${Region}:${Account}:import-task/${ResourceId}`	
export-task	`arn:${Partition}:neptune-graph:${Region}:${Account}:export-task/${ResourceId}`	

Claves de condición para la Analítica de Amazon Neptune

La Analítica de Amazon Neptune define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
neptune-graph:PublicConnectivity	Filtra el acceso según el valor del parámetro de conectividad pública proporcionado en la solicitud o su valor predeterminado, si no se especifica. Todo el acceso a los gráficos se auténtica mediante IAM	Bool

Acciones, recursos y claves de condición para AWS Network Firewall

AWS Network Firewall (prefijo de servicio:`network-firewall`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Network Firewall
- Tipos de recursos definidos por AWS Network Firewall
- Claves de condición para AWS Network Firewall

Acciones definidas por AWS Network Firewall

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptNetworkFirewallTransitGatewayAttachment	Otorga permiso para aceptar los archivos adjuntos pendientes de Network Firewall en una puerta de enlace de tránsito	Escritura	Firewall*		
AssociateAvailabilityZones	Otorga permiso para asociar zonas de disponibilidad a un firewall	Escritura	Firewall*		
AssociateFirewallPolicy	Concede permiso para crear una asociación entre una política de firewall y un firewall	Write	Firewall*		
			FirewallPolicy*		
AssociateSubnets	Concede permiso para asociar subredes de VPC a un firewall	Escritura	Firewall*		
CreateFirewall	Otorga permiso para crear un firewall AWS de Network Firewall	Escritura	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateFirewallPolicy	Otorga permiso para crear una política AWS de firewall de Network Firewall	Escritura	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Otorga permiso para crear un grupo de reglas de AWS Network Firewall	Escritura	StatefulRuleGroup		
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTLSInspectionConfiguration	Otorga permiso para crear una configuración AWS de inspección tls de Network Firewall	Escritura	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcEndpointAssociation	Otorga permiso para crear una asociación de puntos de conexión vpc de AWS Network Firewall	Escritura	Firewall*		iam:CreateServiceLinkedRole
			VpcEndpointAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	Concede permiso para eliminar un firewall	Write	Firewall*		
DeleteFirewallPolicy	Concede permiso para eliminar una política de firewall	Escritura	FirewallPolicy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteNetworkFirewallTransitGatewayAttachment	Otorga permiso para eliminar los archivos adjuntos de Network Firewall en una puerta de enlace de tránsito	Escritura	Firewall*		
DeleteResourcePolicy	Otorga permiso para eliminar una política de recursos para una política de firewall, un grupo de reglas o un firewall	Escritura	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DeleteRuleGroup	Concede permiso para eliminar un grupo de reglas	Escritura	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	Concede permiso para eliminar una configuración de inspección tls	Escritura	TLSInspectionConfiguration*		
DeleteVpcEndpointAssociation	Otorga permiso para eliminar una asociación de puntos de conexión de vpc	Escritura	VpcEndpointAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFirewall	Concede permiso para recuperar los objetos de datos que definen un firewall	Lectura	Firewall*		
DescribeFirewallMetadata	Otorga permiso para recuperar la información de alto nivel sobre un firewall	Lectura	Firewall*		
DescribeFirewallPolicy	Concede permiso para recuperar los objetos de datos que definen una política de firewall	Lectura	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeFlowOperation	Otorga permiso para describir una operación de flujo realizada en un firewall	Lectura	Firewall*		
DescribeLoggingConfiguration	Concede permiso para describir la configuración de registro de un firewall	Lectura	Firewall*		logs:GetLogDelivery logs:ListLogDeliveries

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeResourcePolicy	Otorga permiso para describir una política de recursos para una política, un grupo de reglas o un firewall	Lectura	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroup	Concede permiso para recuperar los objetos de datos que definen un grupo de reglas	Lectura	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupMetadata	Concede permiso para recuperar información de alto nivel sobre un grupo de reglas	Lectura	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	Concede permiso para recuperar los objetos de datos que definen una configuración de inspección tls	Lectura	TLSInspectionConfiguration*		
DescribeVpcEndpointAssociation	Otorga permiso para recuperar los objetos de datos que definen una asociación de puntos de conexión de vpc	Lectura	VpcEndpointAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateAvailabilityZones	Otorga permiso para desasociar las zonas de disponibilidad a un firewall	Escritura	Firewall*		
DisassociateSubnets	Concede permiso para desasociar subredes de VPC de un firewall	Escritura	Firewall*		
GetAnalysisReportResults	Otorga permiso para recuperar los resultados de los informes de análisis de un firewall	Lectura	Firewall*		
ListAnalysisReports	Otorga permiso para enumerar los informes de análisis del firewall	Enumeración	Firewall*		
ListFirewallPolicies	Concede permiso para recuperar los metadatos de las políticas de firewall	List	FirewallPolicy*		
ListFirewalls	Concede permiso para recuperar los metadatos de los firewalls	Enumeración	Firewall*		
ListFlowOperationResults	Otorga permiso para enumerar los resultados de una operación de flujo realizada en un firewall	Lectura	Firewall*		
ListFlowOperations	Otorga permiso para enumerar las operaciones de flujo realizadas en un firewall	Enumeración	Firewall*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRuleGroups	Concede permiso para recuperar los metadatos de los grupos de reglas	Enumeración			
ListTLSInspectionConfigurations	Concede permiso para recuperar los metadatos de la configuración de inspección tls	Enumeración	TLSInspectionConfiguration*		
ListTagsForResource	Concede permiso para recuperar las etiquetas de un recurso	Enumeración	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
ListVpcEndpointAssociations	Otorga permiso para recuperar los metadatos de las asociaciones de puntos finales de vpc	Enumeración	VpcEndpointAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResourcePolicy	Otorga permiso para colocar una política de recursos para una política de firewall, un grupo de reglas o un firewall	Escritura	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
RejectNetworkFirewallTransitGatewayAttachment	Otorga permiso para rechazar los archivos adjuntos pendientes de Network Firewall en una puerta de enlace de tránsito	Escritura	Firewall*		
StartAnalysisReport	Otorga permiso para iniciar un informe de análisis en un firewall	Escritura	Firewall*		
StartFlowCapture	Otorga permiso para iniciar la operación de captura en un firewall	Escritura	Firewall*		
StartFlowFlush	Otorga permiso para iniciar la operación de limpieza en un firewall	Escritura	Firewall*		
TagResource	Concede permiso para adjuntar etiquetas a un recurso	Etiquetado	Firewall		
			FirewallPolicy		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
				aws:TagKeys	
UpdateAvailabilityZoneChangeProtection	Otorga permiso para añadir o eliminar la protección contra cambios de zona de disponibilidad de un firewall	Escritura	Firewall*		
UpdateFirewallAnalysisSettings	Otorga permiso para modificar la configuración de análisis de un firewall	Escritura	Firewall*		
UpdateFirewallDeleteProtection	Concede permiso para agregar o eliminar protección contra eliminaciones de un firewall	Write	Firewall*		
UpdateFirewallDescription	Concede permiso para modificar la descripción de un firewall	Escritura	Firewall*		
UpdateFirewallEncryptionConfiguration	Otorga permiso para modificar la configuración de registro de un firewall	Escritura	Firewall*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFirewallPolicy	Concede permiso para modificar una política de firewall	Write	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	Concede permiso para agregar o eliminar protección contra cambios de política de firewall para un firewall	Write	Firewall*		
UpdateLoggingConfiguration	Concede permiso para modificar la configuración de registro de un firewall	Write	Firewall*		
UpdateRuleGroup	Concede permiso para modificar un grupo de reglas	Write	StatefulRuleGroup		
			StatelessRuleGroup		
UpdateSubnetChangeProtection	Concede permiso para agregar o eliminar protección contra cambios de subred para un firewall	Escritura	Firewall*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTLSInspectionConfiguration	Concede permiso para modificar una configuración de inspección tls	Escritura	TLSInspectionConfiguration*		

Tipos de recursos definidos por AWS Network Firewall

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Firewall	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall/${Name}`	aws:ResourceTag/${TagKey}
FirewallPolicy	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall-policy/${Name}`	aws:ResourceTag/${TagKey}
StatefulRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateful-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
StatelessRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateless-rulegroup/${Name}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
TLSInspectionConfiguration	`arn:${Partition}:network-firewall:${Region}:${Account}:tls-configuration/${Name}`	aws:ResourceTag/${TagKey}
VpcEndpointAssociation	`arn:${Partition}:network-firewall:${Region}:${Account}:vpc-endpoint-association/${Name}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Network Firewall

AWS Network Firewall define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Claves de acciones, recursos y condición del Monitor de flujo de red

Network Flow Monitor (prefijo de servicio:`networkflowmonitor`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el monitor de flujo de red
- Tipos de recursos definidos por Network Flow Monitor
- Claves de condición del monitor de flujo de red

Acciones definidas por el monitor de flujo de red

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMonitor	Otorga permiso para crear un monitor	Escritura	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateScope	Otorga permiso para crear un ámbito	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	Otorga permiso para eliminar un monitor	Escritura	monitor*		
DeleteScope	Otorga permiso para eliminar un ámbito	Escritura	scope*		
GetMonitor	Otorga permiso para obtener información sobre un monitor	Lectura	monitor*		
GetQueryResultsMonitorTopContributors	Otorga permiso para obtener los resultados de una consulta que recupera los datos de los principales colaboradores para un monitor	Lectura	monitor*		
GetQueryResultsWorkloadInsightsTopContributors	Otorga permiso para obtener los resultados de una consulta que recupera los principales colaboradores para obtener información sobre la carga de trabajo	Lectura	scope*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueryResultsWorkloadInsightsTopContributorsData	Otorga permiso para obtener los resultados de una consulta que recupera los puntos de datos de los principales contribuyentes para obtener información sobre la carga de trabajo	Lectura	scope*		
GetQueryStatusMonitorTopContributors	Otorga permiso para obtener el estado de una consulta que recupera los datos de los principales contribuyentes para un monitor	Lectura	monitor*		
GetQueryStatusWorkloadInsightsTopContributors	Otorga permiso para obtener el estado de una consulta que recupera los principales colaboradores para obtener información sobre la carga de trabajo	Lectura	scope*		
GetQueryStatusWorkloadInsightsTopContributorsData	Otorga permiso para obtener el estado de una consulta que recupera los puntos de datos de los principales contribuyentes para obtener información sobre la carga de trabajo	Lectura	scope*		
GetScope	Otorga permiso para obtener información sobre un ámbito	Lectura	scope*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMonitors	Otorga permiso para enumerar todos los monitores de una cuenta y sus estados	Enumeración			
ListScopes	Otorga permiso para obtener todos los ámbitos de una cuenta	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	monitor scope		
Publish	Otorga permiso para publicar un informe	Escritura			
StartQueryMonitorTopContributors	Otorga permiso para iniciar una consulta con el fin de recuperar los datos de los principales colaboradores para un monitor	Escritura	monitor*		
StartQueryWorkloadInsightsTopContributors	Otorga permiso para iniciar una consulta con el fin de recuperar los datos de los principales colaboradores a fin de obtener información sobre la carga de trabajo	Escritura	scope*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartQueryWorkloadInsightsTopContributorsData	Otorga permiso para iniciar una consulta con el fin de recuperar los puntos de datos de los principales contribuyentes para obtener información sobre la carga de trabajo	Escritura	scope*		
StopQueryMonitorTopContributors	Otorga permiso para detener una consulta destinada a recuperar los datos de los principales colaboradores para un monitor	Escritura	monitor*		
StopQueryWorkloadInsightsTopContributors	Otorga permiso para detener una consulta con el fin de recuperar información sobre los principales colaboradores a fin de obtener información sobre la carga de trabajo	Escritura	scope*		
StopQueryWorkloadInsightsTopContributorsData	Otorga permiso para detener una consulta con el fin de recuperar los puntos de datos de los principales contribuyentes para obtener información sobre la carga de trabajo	Escritura	scope*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	monitor scope		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	monitor		
			scope		
				aws:TagKeys	
UpdateMonitor	Otorga permiso para actualizar un monitor	Escritura	monitor*		
UpdateScope	Otorga permiso para actualizar un ámbito	Escritura	scope*		

Tipos de recursos definidos por Network Flow Monitor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
monitor	`arn:${Partition}:networkflowmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
scope	`arn:${Partition}:networkflowmonitor:${Region}:${Account}:scope/${ScopeId}`	aws:ResourceTag/${TagKey}

Claves de condición del monitor de flujo de red

El monitor de flujo de red define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares clave-valor de la etiqueta en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra las acciones mediante las claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para el Administrador de red de AWS

AWS Network Manager (prefijo de servicio:`networkmanager`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el administrador de red de AWS
- Tipos de recurso definidos por el administrador de red de AWS
- Claves de condición para el administrador de red de AWS

Acciones definidas por el administrador de red de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptAttachment	Concede permiso para aceptar la creación de un adjunto entre un origen y un destino en una red principal.	Escritura	attachment*		ec2:DescribeRegions
AssociateConnectPeer	Concede permiso para asociar un Connect Peer.	Escritura	device*		
			global-network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateCustomerGateway	Concede permiso para asociar una gateway de cliente a un dispositivo	Write	device*		
			global-network*		
			link		
				networkmanager:cgwArn	
AssociateLink	Concede permiso para asociar un vínculo a un dispositivo.	Write	device*		
			global-network*		
			link*		
AssociateTransitGatewayConnectPeer	Concede el permiso para asociar un par de conexión de puerta de enlace de tránsito a un dispositivo.	Escritura	device*		
			global-network*		
			link		
				networkmanager:tgwConnectPeerArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnectAttachment	Concede permiso para crear un adjunto Connect.	Escritura	attachment*		ec2:DescribeRegions networkmanager:TagResource
			core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectPeer	Concede permiso para crear una conexión Connect Peer.	Escritura	attachment*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnection	Concede permiso para crear una conexión nueva.	Escritura	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetwork	Concede permiso para crear una red principal nueva.	Escritura	global-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDevice	Concede permiso para crear un dispositivo nuevo.	Escritura	global-network*		networkmanager:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAttachment	Otorga permiso para crear un adjunto a la puerta de enlace Direct Connect	Escritura	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:directConnectGatewayArn networkmanager:edgeLocations	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGlobalNetwork	Concede permiso para crear una red global nueva.	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole networkmanager:TagResource
CreateLink	Concede permiso para crear un enlace nuevo.	Write	global-network*		networkmanager:TagResource
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSite	Concede permiso para crear un sitio nuevo.	Escritura	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSiteToSiteVpnAttachment	Otorga permiso para crear un adjunto de site-to-site VPN	Escritura	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpnConnectionArn	
CreateTransitGatewayPeering	Otorga permiso para crear un emparejamiento de Transit Gateway.	Escritura	core-network*		ec2:DescribeRegions networkmanager:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwArn	
CreateTransitGatewayRouteTableAttachment	Otorga permiso para crear una conexión de tabla de enrutamiento de Transit Gateway.	Escritura	peering*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwRtbArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVpcAttachment	Concede permiso para crear un adjunto VPC.	Escritura	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpcArn networkmanager:subnetArns	
DeleteAttachment	Concede permiso para eliminar un adjunto.	Escritura	attachment*		ec2:DescribeRegions
DeleteConnectPeer	Concede permiso para eliminar un Connect Peer.	Escritura	connect-peer*		ec2:DescribeRegions
DeleteConnection	Concede permiso para eliminar una conexión.	Escritura	connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			global-network*		
DeleteCoreNetwork	Concede permiso para eliminar una red principal.	Escritura	core-network*		ec2:DescribeRegions
DeleteCoreNetworkPolicyVersion	Concede permiso para eliminar la versión principal de la política de red.	Escritura	core-network*		
DeleteDevice	Concede permiso para eliminar un dispositivo.	Write	device*		
			global-network*		
DeleteGlobalNetwork	Concede permiso para eliminar una red global.	Write	global-network*		
DeleteLink	Concede permisos para eliminar un enlace.	Escritura	global-network*		
			link*		
DeletePeering	Otorga permiso para eliminar un emparejamiento.	Escritura	peering*		ec2:DescribeRegions
DeleteResourcePolicy	Concede permiso para eliminar un recurso.	Escritura	core-network*		
DeleteSite	Concede permiso para eliminar un sitio	Write	global-network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			site*		
DeregisterTransitGateway	Concede permiso para anular el registro de una gateway de tránsito de una red global.	Write	global-network*		
				networkmanager:tgwArn	
DescribeGlobalNetworks	Concede permiso para describir redes globales.	Enumeración	global-network		
DisassociateConnectPeer	Concede permiso para disociar un Connect Peer.	Escritura	global-network*		
DisassociateCustomerGateway	Concede permiso para desasociar una gateway de cliente de un dispositivo.	Write	global-network*		
				networkmanager:cgwArn	
DisassociateLink	Concede permiso para desasociar un enlace de un dispositivo.	Write	device*		
			global-network*		
			link*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateTransitGatewayConnectPeer	Concede el permiso para desasociar un par de conexión de puerta de enlace de tránsito de un dispositivo.	Escritura	global-network*		
				networkmanager:tgwConnectPeerArn	
ExecuteCoreNetworkChangeSet	Concede permiso para aplicar cambios en la red principal.	Escritura	core-network*		ec2:DescribeRegions
GetConnectAttachment	Concede permiso para recuperar un adjunto Connect.	Lectura	attachment*		
GetConnectPeer	Concede permiso para recuperar un Connect Peer.	Lectura	connect-peer*		
GetConnectPeerAssociations	Concede permiso para describir asociaciones de Connect Peer.	Lectura	global-network*		
GetConnections	Concede el permiso para describir conexiones.	Enumeración	global-network*		
			connection		
GetCoreNetwork	Concede permiso para recuperar una red principal.	Lectura	core-network*		
GetCoreNetworkChangeEvents	Otorga permiso para recuperar una lista de eventos de cambios de red principal.	Lectura	core-network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCoreNetworkChangeSet	Concede permiso para recuperar una lista de conjuntos de cambios de red principal.	Lectura	core-network*		
GetCoreNetworkPolicy	Concede permiso para recuperar la política de red principal.	Lectura	core-network*		
GetCustomerGatewayAssociations	Concede permiso para describir asociaciones de gateway de clientes.	List	global-network*		
GetDevices	Concede permiso para describir dispositivos.	Enumeración	global-network*		
			device		
GetDirectConnectGatewayAttachment	Otorga permiso para recuperar un adjunto de la puerta de enlace Direct Connect	Lectura	attachment*		
GetLinkAssociations	Concede permiso para describir asociaciones de enlaces.	List	global-network*		
			device		
			link		
GetLinks	Concede permiso para describir enlaces.	Enumeración	global-network*		
			link		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetNetworkResourceCounts	Concede permiso para devolver el número de recursos de una red global agrupada por tipo.	Lectura	global-network*		
GetNetworkResourceRelationships	Concede permiso para recuperar recursos relacionados de un recurso de red global.	Lectura	global-network*		
GetNetworkResources	Concede permiso para recuperar un recurso de red global.	Lectura	global-network*		
GetNetworkRoutes	Concede permiso para recuperar rutas para una tabla de enrutamiento dentro de la red global.	Lectura	global-network*		
GetNetworkTelemetry	Concede permiso para recuperar objetos de telemetría de red para red global.	Lectura	global-network*		
GetResourcePolicy	Concede permiso para recuperar una política de recursos.	Lectura	core-network*		
GetRouteAnalysis	Concede permiso para recuperar una configuración y un resultado de análisis de ruta.	Lectura	global-network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSiteToSiteVpnAttachment	Otorga permiso para recuperar un archivo adjunto de la site-to-site VPN	Lectura	attachment*		
GetSites	Concede permiso para describir redes globales.	List	global-network*		
			site		
GetTransitGatewayConnectPeerAssociations	Concede el permiso para describir asociaciones de pares de conexión de puerta de enlace de tránsito.	Enumeración	global-network*		
GetTransitGatewayPeering	Otorga permiso para recuperar un emparejamiento de Transit Gateway.	Lectura	peering*		
GetTransitGatewayRegistrations	Concede permiso para describir los registros de gateway de tránsito.	Enumeración	global-network*		
GetTransitGatewayRouteTableAttachment	Otorga permiso para recuperar una conexión de tabla de enrutamiento de Transit Gateway.	Lectura	attachment*		
GetVpcAttachment	Concede permiso para recuperar un adjunto de VPC.	Lectura	attachment*		
ListAttachments	Concede permiso para describir archivos adjuntos.	Enumeración	attachment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConnectPeers	Concede permiso para describir Connect Peers.	Enumeración	connect-peer*		
ListCoreNetworkPolicyVersions	Concede permiso para enumerar versiones principales de la política de red.	Enumeración	core-network*		
ListCoreNetworks	Concede permiso para enumerar redes principales.	Enumeración			
ListOrganizationServiceAccessStatus	Concede permiso para ver una lista del estado de acceso a los servicios de la organización	Enumeración			
ListPeerings	Otorga el permiso para describir emparejamientos.	Enumeración			
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso del administrador de red.	Lectura	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			link		
			peering		
			site		
				aws:ResourceTag/${TagKey}	
PutCoreNetworkPolicy	Concede permiso para crear una política principal de red.	Escritura	core-network*		ec2:DescribeRegions
PutResourcePolicy	Concede permiso para crear o actualizar una política de recursos.	Escritura	core-network*		
RegisterTransitGateway	Concede permiso para registrar una gateway de tránsito en una red global.	Escritura	global-network*		
				networkmanager:tgwArn	
RejectAttachment	Concede permiso para rechazar la solicitud de adjuntos.	Escritura	attachment*		
RestoreCoreNetworkPolicyVersion	Concede permiso para restaurar la política de red principal a una versión anterior.	Escritura	core-network*		ec2:DescribeRegions

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartOrganizationServiceAccessUpdate	Concede permiso para iniciar la actualización del acceso a los servicios de la organización	Escritura			
StartRouteAnalysis	Concede permiso para iniciar un análisis de rutas y almacena una configuración de análisis.	Escritura	global-network*		
TagResource	Concede permiso para etiquetar un recurso del administrador de red.	Etiquetado	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para desetiquetar un recurso del administrador de red.	Etiquetado	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateConnection	Concede permiso para actualizar una conexión.	Escritura	connection*		
			global-network*		
UpdateCoreNetwork	Concede permiso para actualizar una red principal.	Escritura	core-network*		
UpdateDevice	Concede permiso para actualizar un dispositivo.	Escritura	device*		
			global-network*		
UpdateDirectConnectGatewayAttachment	Otorga permiso para actualizar un adjunto de la puerta de enlace Direct Connect	Escritura	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:edgeLocations	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGlobalNetwork	Concede permiso para actualizar una red global.	Write	global-network*		
UpdateLink	Concede permiso para actualizar un enlace.	Escritura	global-network*		
			link*		
UpdateNetworkResourceMetadata	Otorga permiso para agregar o actualizar key/value pares de metadatos en un recurso de red	Escritura	global-network*		
UpdateSite	Concede permiso para actualizar un sitio	Escritura	global-network*		
			site*		
UpdateVpcAttachment	Concede permiso para actualizar un adjunto de VPC.	Escritura	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:subnetArns	

Tipos de recurso definidos por el administrador de red de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
global-network	`arn:${Partition}:networkmanager::${Account}:global-network/${ResourceId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:networkmanager::${Account}:site/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
link	`arn:${Partition}:networkmanager::${Account}:link/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:networkmanager::${Account}:device/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
connection	`arn:${Partition}:networkmanager::${Account}:connection/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
core-network	`arn:${Partition}:networkmanager::${Account}:core-network/${ResourceId}`	aws:ResourceTag/${TagKey}
attachment	`arn:${Partition}:networkmanager::${Account}:attachment/${ResourceId}`	aws:ResourceTag/${TagKey}
connect-peer	`arn:${Partition}:networkmanager::${Account}:connect-peer/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
peering	`arn:${Partition}:networkmanager::${Account}:peering/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para el administrador de red de AWS

AWS Network Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
networkmanager:cgwArn	Filtra el acceso mediante qué puertas de enlace de cliente se pueden asociar o disociar.	ARN
networkmanager:directConnectGatewayArn	Filtra el acceso mediante el cual se puede usar la puerta de enlace Direct Connect a un create/update archivo adjunto	ARN

Claves de condición	Descripción	Tipo
networkmanager:edgeLocations	Filtra el acceso mediante el cual se pueden agregar o quitar ubicaciones de borde de un adjunto de puerta de enlace Direct Connect	ArrayOfString
networkmanager:subnetArns	Filtra el acceso mediante qué subredes de VPC pueden agregarse o eliminarse de un adjunto de VPC.	ArrayOfARN
networkmanager:tgwArn	Filtra el acceso mediante el cual las puertas de enlace de tránsito se pueden registrar, anular su registro o emparejar.	ARN
networkmanager:tgwConnectPeerArn	Filtra el acceso mediante qué pares de conexión de puerta de enlace pueden asociarse o disociarse.	ARN
networkmanager:tgwRtbArn	Filtra el acceso mediante el cual se puede usar la tabla de enrutamiento de Transit Gateway para crear una conexión	ARN
networkmanager:vpcArn	Filtra el acceso mediante el cual se puede usar la VPC a un archivo adjunto create/update	ARN
networkmanager:vpnConnectionArn	Filtra el acceso mediante el cual se puede usar la Site-to-Site VPN a un archivo adjunto create/update	ARN

Acciones, recursos y claves de condición para el chat del Administrador de red de AWS

AWS Network Manager Chat (prefijo de servicio:`networkmanager-chat`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el chat del administrador de red de AWS
- Tipos de recurso definidos por el chat del administrador de red de AWS
- Claves de condición para el chat del administrador de red de AWS

Acciones definidas por el chat del administrador de red de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelMessageResponse [solo permiso]	Otorga permiso para cancelar una respuesta a un mensaje	Escritura			
CreateConversation [solo permiso]	Concede permiso para crear una conversación	Escritura			
DeleteConversation [solo permiso]	Concede permiso para eliminar una conversación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConversationMessages [solo permiso]	Concede permiso para enumerar los mensajes de conversiones	Enumeración			
ListConversations [solo permiso]	Concede permiso para enumerar las conversiones	Enumeración			
NotifyConversationIsActive [solo permiso]	Concede permiso para notificar si hay actividad en una conversación	Escritura			
SendConversationMessage [solo permiso]	Concede permiso para enviar un mensaje en una conversación	Escritura			

Tipos de recurso definidos por el chat del administrador de red de AWS

AWS Network Manager Chat no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir que obtenga acceso al chat del administrador de red de AWS , especifique `"Resource": "*"` en su política.

Claves de condición para el chat del administrador de red de AWS

El chat del administrador de red no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Nimble Studio

Amazon Nimble Studio (prefijo de servicio: `nimble`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Nimble Studio
- Tipos de recursos definidos por Amazon Nimble Studio
- Claves de condición de Amazon Nimble Studio

Acciones definidas por Amazon Nimble Studio

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptEulas	Otorga permiso para aceptar EULAs	Escritura	eula*		
CreateLaunchProfile	Concede permiso para crear un perfil de inicio	Write	studio*		ec2:CreateNetworkInterface ec2:DescribeNatGateways

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:RunInstances
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateStreamingImage	Concede permiso para crear una imagen de streaming	Write	studio*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateStreamingSession	Concede permiso para crear una sesión de streaming	Escritura	launch-profile*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission nimble:GetLaunchProfile nimble:GetLaunchProfileInitialization nimble:ListEulaAcceptances
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSessionStream	Otorga permiso para crear un StreamingSessionStream	Escritura	streaming-session*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				nimble:requesterPrincipalId	
CreateStudio	Concede permiso para crear un estudio	Write	studio*		iam:PassRole sso:CreateManagedApplicationInstance
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateStudioComponent	Concede permiso para crear un componente de estudio. Un componente de estudio designa un recurso de red al que un perfil de lanzamiento proporcionará acceso	Write	studio*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLaunchProfile	Concede permiso para eliminar un perfil de inicio	Write	launch-profile*		
DeleteLaunchProfileMember	Concede permiso para eliminar un miembro de perfil de inicio	Write	launch-profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteStreamingImage	Concede permiso para eliminar una imagen de streaming	Write	streaming-image*		ec2:DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute
DeleteStreamingSession	Concede permiso para eliminar una sesión de streaming	Write	streaming-session*		ec2:DeleteNetworkInterface
				nimble:requesterPrincipalId	
DeleteStudio	Concede permiso para eliminar un estudio	Write	studio*		sso:DeleteManagedApplicationInstance
DeleteStudioComponent	Concede permiso para eliminar un componente de estudio	Write	studio-component*		ds:UnauthorizeApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteStudioMember	Concede permiso para eliminar un miembro de estudio	Write	studio*		
GetEula	Concede permiso para obtener un CLUF	Read	eula*		
GetFeatureMap [solo permiso]	Concede permiso con el fin de que el portal de Nimble Studio muestre las características adecuadas para esta cuenta	Read			
GetLaunchProfile	Concede permiso para obtener un perfil de lanzamiento	Read	launch-profile*		
GetLaunchProfileDetails	Concede permiso para obtener los detalles de un perfil de lanzamiento, que incluye el resumen de los componentes de estudio y las imágenes de streaming utilizadas por el perfil de lanzamiento	Read	launch-profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLaunchProfileInitialization	Concede permiso para obtener una inicialización de perfil de lanzamiento. Una inicialización de perfil de lanzamiento es una versión desreferenciada de un perfil de lanzamiento, incluida la información de conexión de componentes de estudio adjuntos	Read	launch-profile*		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	Concede permiso para obtener un miembro del perfil de lanzamiento	Read	launch-profile*		
GetStreamingImage	Concede permiso para obtener una imagen en streaming	Read	streaming-image*		
GetStreamingSession	Concede permiso para obtener una sesión de streaming	Lectura	streaming-session*		
				nimble:requesterPrincipalId	
GetStreamingSessionBackup	Concede permiso para obtener una copia de seguridad de una sesión de streaming	Lectura	streaming-session-backup*		
				nimble:requesterPrincipalId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetStreamingSessionStream	Concede permiso para obtener una secuencia de sesión de streaming	Read	streaming-session*		
				nimble:requesterPrincipalId	
GetStudio	Concede permiso para obtener un estudio	Read	studio*		
GetStudioComponent	Concede permiso para obtener un componente de estudio	Read	studio-component*		
GetStudioMember	Concede permiso para obtener un miembro del estudio	Read	studio*		
ListEulaAcceptances	Concede permiso para enumerar las aceptaciones del CLUF	Lectura	eula-acceptance*		
ListEulas	Otorga permiso para publicar EULAs	Lectura	eula*		
ListLaunchProfileMembers	Concede permiso para enumerar miembros del perfil de lanzamiento	Read	launch-profile*		
ListLaunchProfiles	Concede permiso para enumerar perfiles de lanzamiento	Read	studio*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				nimble:principalId nimble:requesterPrincipalId	
ListStreamingImages	Concede permiso para enumerar imágenes de streaming	Lectura	studio*		
ListStreamingSessionBackups	Concede permiso para enumerar las copias de seguridad de sesiones de streaming	Lectura	studio*		
				nimble:requesterPrincipalId	
ListStreamingSessions	Concede permiso para enumerar sesiones de streaming	Read	studio*		
				nimble:createdBy nimble:ownedBy nimble:requesterPrincipalId	
ListStudioComponents	Concede permiso para enumerar los componentes de estudio	Read	studio*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStudioMembers	Concede permiso para enumerar miembros del estudio	Read	studio*		
ListStudios	Concede permiso para enumerar todos los estudios	Read			
ListTagsForResource	Concede permiso para enumerar todas las etiquetas en un recurso de Nimble Studio	Lectura	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
PutLaunchProfileMembers	Otorga permiso para add/update lanzar miembros del perfil	Escritura	launch-profile*		sso-directory:DescribeUsers
PutStudioLogEvents [solo permiso]	Concede permiso con el fin de informar de métricas y registros para que el portal de Nimble Studio monitoree el estado de la aplicación	Escritura	studio*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutStudioMembers	Otorga permiso a los miembros del add/update estudio	Escritura	studio*		sso-directory:DescribeUsers
StartStreamingSession	Concede permiso para iniciar una sesión de streaming.	Escritura	streaming-session*		nimble:GetLaunchProfile nimble:GetLaunchProfileMember
			streaming-session-backup		
				nimble:requesterPrincipalId	
StartStudioSSOConfigurationRepair	Otorga permiso para reparar la configuración del AWS IAM Identity Center del estudio	Escritura	studio*		sso:CreateManagedApplicationInstance sso:GetManagedApplicationInstance

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopStreamingSession	Concede permiso para detener una sesión de streaming.	Escritura	streaming-session*		nimble:GetLaunchProfile
				nimble:requesterPrincipalId	
TagResource	Concede permiso con el fin de agregar o sobrescribir una o más etiquetas para el recurso de Nimble Studio especificado	Etiquetado	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para desasociar una o más etiquetas del recurso de Nimble Studio especificado	Etiquetado	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateLaunchProfile	Concede permiso para actualizar un perfil de lanzamiento	Write	launch-profile*		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	Concede permiso para actualizar un miembro de perfil de lanzamiento	Write	launch-profile*		
UpdateStreamingImage	Concede permiso para actualizar una imagen de streaming	Write	streaming-image*		
UpdateStudio	Concede permiso para actualizar un estudio	Write	studio*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateStudioComponent	Concede permiso para actualizar un componente de estudio	Write	studio-component*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

Tipos de recursos definidos por Amazon Nimble Studio

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
studio	`arn:${Partition}:nimble:${Region}:${Account}:studio/${StudioId}`	aws:RequestTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
		aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
streaming-image	arn:${Partition}:nimble:${Region}:${Account}:streaming-image/${StreamingImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
studio-component	arn:${Partition}:nimble:${Region}:${Account}:studio-component/${StudioComponentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
launch-profile	arn:${Partition}:nimble:${Region}:${Account}:launch-profile/${LaunchProfileId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId

Tipos de recurso	ARN	Claves de condición
streaming-session	arn:${Partition}:nimble:${Region}:${Account}:streaming-session/${StreamingSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:createdBy nimble:ownedBy
streaming-session-backup	arn:${Partition}:nimble:${Region}:${Account}:streaming-session-backup/${StreamingSessionBackupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:ownedBy
eula	arn:${Partition}:nimble:${Region}:${Account}:eula/${EulaId}	
eula-acceptance	arn:${Partition}:nimble:${Region}:${Account}:eula-acceptance/${EulaAcceptanceId}	nimble:studioId

Claves de condición de Amazon Nimble Studio

Amazon Nimble Studio define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
nimble:createdBy	Filtra el acceso mediante el parámetro de solicitud createdBy o el ID del creador del recurso.	Cadena
nimble:ownedBy	Filtra el acceso mediante el parámetro de solicitud ownedBy o el ID del propietario del recurso.	Cadena
nimble:principalId	Filtra el acceso mediante el parámetro de solicitud principalId.	Cadena
nimble:requesterPrincipalId	Filtra el acceso mediante el ID del usuario que ha iniciado sesión.	Cadena
nimble:studioId	Filtra el acceso mediante un estudio específico.	ARN

Acciones, recursos y claves de condición para Amazon One Enterprise

Amazon One Enterprise (prefijo de servicio: one) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon One Enterprise
- Tipos de recurso definidos por Amazon One Enterprise
- Claves de condición de Amazon One Enterprise

Acciones definidas por Amazon One Enterprise

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeviceActivationQrCode	Concede permiso para crear un código QR para una instancia de dispositivo	Escritura	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateDeviceConfigurationTemplate	Concede permiso para crear una plantilla de configuración del dispositivo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDeviceInstance	Concede permiso para crear una instancia del dispositivo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstanceConfiguration	Concede permiso para crear la configuración de una instancia del dispositivo	Escritura	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateSite	Concede permiso para crear un sitio	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssociatedDevice	Concede permiso para desasociar un dispositivo de una instancia del dispositivo	Escritura	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceConfigurationTemplate	Concede permiso para eliminar una plantilla de configuración del dispositivo	Escritura	device-configuration-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeleteDeviceInstance	Concede permiso para eliminar una instancia del dispositivo	Escritura	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteSite	Concede permiso para eliminar un sitio	Escritura	site*		
				aws:ResourceTag/${TagKey}	
DeleteUserV1	Concede permiso para eliminar un usuario	Escritura	user*		
GetDeviceConfigurationTemplate	Concede permiso para ver una plantilla de configuración del dispositivo	Lectura	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstance	Concede permiso para ver una instancia de dispositivo	Lectura	device-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetDeviceInstanceConfiguration	Concede permiso para ver la configuración de una instancia del dispositivo	Lectura	configuration*		
				aws:ResourceTag/${TagKey}	
GetSite	Concede permiso para ver un sitio	Lectura	site*		
				aws:ResourceTag/${TagKey}	
GetSiteAddress	Concede permiso para ver la dirección de un sitio	Lectura	site*		
				aws:ResourceTag/${TagKey}	
ListDeviceConfigurationTemplates	Concede permiso para recuperar la lista de plantillas de configuración del dispositivo	Enumeración			
ListDeviceInstances	Concede permiso para recuperar una lista de instancias de dispositivos	Enumeración			
ListSites	Concede permiso para ver una lista de los sitios	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso de Amazon One Enterprise	Lectura	device-configuration-template		
			device-instance		
			site		
				aws:ResourceTag/${TagKey}	
ListUsersV1	Concede permiso para ver la lista de usuarios	Enumeración			
RebootDevice	Concede permiso para reiniciar el dispositivo asociado a una instancia de dispositivo	Escritura	device-instance*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para agregar etiquetas a un recurso de Amazon One Enterprise	Etiquetado	device-configuration-template		
			device-instance		
			site		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso de Amazon One Enterprise	Etiquetado	device-configuration-template		
			device-instance		
			site		
				aws:TagKeys	
UpdateDeviceConfigurationTemplate	Concede permiso para actualizar una plantilla de configuración del dispositivo	Escritura	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
UpdateDeviceInstance	Concede permiso para actualizar una instancia del dispositivo	Escritura	device-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateSite	Concede permiso para actualizar un sitio	Escritura	site*		
				aws:ResourceTag/${TagKey}	
UpdateSiteAddress	Concede permiso para actualizar la dirección de un sitio	Escritura	site*		
				aws:ResourceTag/${TagKey}	

Tipos de recurso definidos por Amazon One Enterprise

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
device-instance	`arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
configuration	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}/configuration/${Version}	
device-configuration-template	arn:${Partition}:one:${Region}:${Account}:device-configuration-template/${TemplateId}	aws:ResourceTag/${TagKey}
site	arn:${Partition}:one:${Region}:${Account}:site/${SiteId}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:one:${Region}:${Account}:user/${UserId}	

Claves de condición de Amazon One Enterprise

Amazon One Enterprise define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante los pares de clave-valor de etiqueta de la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante los pares de clave-valor de etiqueta asociados al recurso.	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon OpenSearch

Amazon OpenSearch (prefijo de servicio:`opensearch`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon OpenSearch
- Tipos de recursos definidos por Amazon OpenSearch
- Claves de estado de Amazon OpenSearch

Acciones definidas por Amazon OpenSearch

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso

que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ApplicationAccessAll [solo permiso]	Otorga permiso para acceder a la aplicación OpenSearch	Administración de permisos	application*		
CancelDirectQuery	Otorga permiso para cancelar la consulta que se envía al OpenSearch DataSource recurso	Escritura	datasource*		
GetDirectQuery	Otorga permiso para obtener el estado de las consultas que se realizan en el OpenSearch DataSource recurso	Lectura	datasource*		
GetDirectQueryResult	Otorga permiso para obtener los resultados de una consulta que se realiza en el OpenSearch DataSource recurso	Lectura	datasource*		
StartDirectQuery	Otorga permiso para iniciar una consulta directa en los OpenSearch DataSource arns proporcionados	Escritura	datasource*		

Tipos de recursos definidos por Amazon OpenSearch

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}`	
datasource	`arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}`	

Claves de estado de Amazon OpenSearch

OpenSearch no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones de Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion (prefijo de servicio:`osis`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon OpenSearch Ingestion

- Tipos de recursos definidos por Amazon OpenSearch Ingestion
- Claves de estado de Amazon OpenSearch Ingestion

Acciones definidas por Amazon OpenSearch Ingestion

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePipeline	Otorga permiso para crear una canalización de OpenSearch ingestión	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:CreateLogDelivery
DeletePipeline	Otorga permiso para eliminar una canalización de OpenSearch ingestión	Escritura	pipeline*		logs:DeleteLogDelivery logs:GetLogDelivery

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					logs:ListLogDeliveries
GetPipeline	Otorga permiso para recuperar la información de configuración de una canalización de OpenSearch ingestión	Lectura	pipeline*		
GetPipelineBlueprint	Otorga permiso para obtener el contenido de un plano de canalización de OpenSearch Ingestion	Lectura	pipeline-blueprint*		
GetPipelineChangeProgress	Otorga permiso para obtener información detallada sobre el estado de una canalización de ingestion OpenSearch	Lectura	pipeline*		
Ingest	Otorga permiso para ingerir datos a través de una OpenSearch canalización de ingestión	Escritura	pipeline*		
ListPipelineBlueprints	Otorga permiso para enumerar los nombres de los planos disponibles para una OpenSearch configuración de canalización de ingestión	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPipelines	Otorga permiso para incluir la configuración básica de cada canalización OpenSearch de ingestión de la cuenta corriente y la región	Enumeración			
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas de recursos asociadas a una canalización de OpenSearch ingestion	Lectura	pipeline*		
StartPipeline	Otorga permiso para iniciar una canalización de OpenSearch ingestión	Escritura	pipeline*		
StopPipeline	Otorga permiso para detener una canalización de OpenSearch ingestión	Escritura	pipeline*		
TagResource	Otorga permiso para adjuntar etiquetas de recursos a una canalización de OpenSearch ingestión	Etiquetado	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de recursos de una canalización del servicio OpenSearch de ingestión	Etiquetado	pipeline*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePipeline	Otorga permiso para modificar la configuración de una canalización de OpenSearch ingestión	Escritura	pipeline*		iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
ValidatePipeline	Otorga permiso para validar la configuración de una canalización de OpenSearch ingestión	Lectura			

Tipos de recursos definidos por Amazon OpenSearch Ingestion

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
pipeline	`arn:${Partition}:osis:${Region}:${Account}:pipeline/${PipelineName}`	aws:ResourceTag/${TagKey}
pipeline-blueprint	`arn:${Partition}:osis:${Region}:${Account}:blueprint/${BlueprintName}`	

Claves de estado de Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon OpenSearch Serverless

Amazon OpenSearch Serverless (prefijo de servicio:`aoss`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon OpenSearch Serverless
- Tipos de recursos definidos por Amazon OpenSearch Serverless
- Claves de condición de Amazon OpenSearch Serverless

Acciones definidas por Amazon OpenSearch Serverless

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
APIAccessAll	Concede permiso a todos los Opensearch compatibles APIs	Escritura	Collection*		
				aoss:collection aoss:CollectionId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetCollection	Otorga permiso para obtener los atributos de una o varias colecciones	Lectura		aoss:collection	
BatchGetEffectiveLifecyclePolicy	Concede permiso para obtener información sobre una política de ciclo de vida aplicada a uno o más recursos de AOSS	Lectura			
BatchGetLifecyclePolicy	Concede permiso para obtener información acerca de una o varias políticas de ciclo de vida	Lectura			
BatchGetVpcEndpoint	Otorga permiso para obtener uno o varios puntos de conexión de VPC	Lectura			
CreateAccessPolicy	Otorga permiso para crear una política de acceso a datos	Escritura		aoss:collection aoss:index	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCollection	Otorga permiso para crear una colección sin servidor	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateLifecyclePolicy	Concede permiso para crear una política de ciclo de vida	Escritura		aoss:index	
CreateSecurityConfig	Otorga permiso para crear una configuración de seguridad sin servidor	Escritura			
CreateSecurityPolicy	Otorga permiso para crear una política de red o cifrado	Escritura		aoss:collection	
CreateVpcEndpoint	Concede permiso para crear un punto final OpenSearch-Serverless-managed de VPC de interfaz	Escritura			
DashboardsAccessAll	Concede permiso para OpenSearch Serverless Dashboards	Escritura	Dashboards*		
				aoss:collection aoss:CollectionId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccessPolicy	Otorga permiso para eliminar una política de acceso a datos	Escritura		aoss:collection aoss:index	
DeleteCollection	Otorga permiso para eliminar una colección sin servidor	Escritura	Collection*		
DeleteLifecyclePolicy	Concede permiso para eliminar una política de ciclo de vida	Escritura		aoss:index	
DeleteSecurityConfig	Concede permiso para eliminar una configuración de seguridad	Escritura			
DeleteSecurityPolicy	Otorga permiso para eliminar una política de seguridad	Escritura		aoss:collection	
DeleteVpcEndpoint	Concede permiso para eliminar un punto final de OpenSearch VPC de interfaz administrada sin servidor	Escritura			
GetAccessPolicy	Otorga permiso para obtener información sobre una política de acceso a datos	Lectura		aoss:collection aoss:index	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountSettings	Otorga permiso para obtener la configuración de la cuenta, incluida la configuración de capacidad	Lectura			
GetPoliciesStats	Otorga permiso para obtener estadísticas sobre las políticas de seguridad de su cuenta	Lectura			
GetSecurityConfig	Otorga permiso para obtener información sobre una configuración de seguridad sin servidor	Lectura			
GetSecurityPolicy	Otorga permiso para obtener información sobre una política de seguridad	Lectura		aoss:collection	
ListAccessPolicies	Otorga permiso para enumerar las políticas de acceso a datos	Enumeración			
ListCollections	Otorga permiso para enumerar las colecciones	Enumeración			
ListLifecyclePolicies	Concede permiso para enumerar las políticas de ciclo de vida	Enumeración			
ListSecurityConfigs	Otorga permiso para enumerar las configuraciones de seguridad	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSecurityPolicies	Otorga permiso para mostrar una lista de políticas de seguridad.	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de una colección	Enumeración			
ListVpcEndpoints	Otorga permiso para enumerar los puntos finales de OpenSearch VPC gestionados sin servidor	Enumeración			
TagResource	Otorga permiso para etiquetar una colección sin servidor	Escritura		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de una colección	Escritura		aws:TagKeys	
UpdateAccessPolicy	Otorga permiso para actualizar una política de acceso a datos	Escritura		aoss:collection aoss:index	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccountSettings	Otorga permiso para actualizar la configuración de la cuenta, incluida la configuración de capacidad	Escritura			
UpdateCollection	Otorga permiso para actualizar una colección	Escritura	Collection*		
UpdateLifecyclePolicy	Concede permiso para actualizar una política de ciclo de vida	Escritura		aoss:index	
UpdateSecurityConfig	Otorga permiso para actualizar una configuración de seguridad	Escritura			
UpdateSecurityPolicy	Otorga permiso para actualizar una política de seguridad	Escritura		aoss:collection	
UpdateVpcEndpoint	Otorga permiso para actualizar un punto final de OpenSearch VPC administrado sin servidor	Escritura			

Tipos de recursos definidos por Amazon OpenSearch Serverless

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Collection	`arn:${Partition}:aoss:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
Dashboards	`arn:${Partition}:aoss:${Region}:${Account}:dashboards/default`	

Claves de condición de Amazon OpenSearch Serverless

Amazon OpenSearch Serverless define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aoss:CollectionId	Filtra el acceso por el identificador de la colección	Cadena
aoss:collection	Filtra el acceso por el nombre de la colección	Cadena
aoss:index	Filtra el acceso por el índice	Cadena
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon OpenSearch Service

Amazon OpenSearch Service (prefijo de servicio:`es`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon OpenSearch Service
- Tipos de recursos definidos por Amazon OpenSearch Service
- Claves de estado de Amazon OpenSearch Service

Acciones definidas por Amazon OpenSearch Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptInboundConnection	Otorga permiso al propietario del dominio de destino para aceptar una solicitud de conexión de búsqueda entre clústeres entrantes	Escritura			
AcceptInboundCrossClusterSe	Otorga permiso al propietario del dominio de destino para aceptar una solicitud de conexión de búsqueda	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
archConnection	entre clústeres entrantes. Este permiso está obsoleto. Úselo AcceptInboundConnection en su lugar				
AddDataSource	Otorga permiso para agregar la fuente de datos para el dominio del OpenSearch servicio	Escritura	domain*		
AddDirectQueryDataSource	Otorga permiso para agregar la fuente de datos para los OpenSearch arns proporcionados	Escritura	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddTags	Otorga permiso para adjuntar etiquetas de recursos a un dominio de OpenSearch servicio, fuente de datos o aplicación	Etiquetado	application*		
			datasource*		
			domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociatePackage	Otorga permiso para asociar un paquete a un dominio OpenSearch de servicio	Escritura	domain*		
AssociatePackages	Otorga permiso para asociar varios paquetes a un dominio OpenSearch de servicio	Escritura	domain*		
AuthorizeVpcEndpointAccess	Otorga permiso para proporcionar acceso a un dominio de Amazon OpenSearch Service mediante el uso de un punto final de interfaz de VPC	Escritura			
CancelDomainConfigChange	Otorga permiso para cancelar un cambio en un dominio OpenSearch de servicio	Escritura	domain*		
CancelElasticsearchServiceSoftwareUpdate	Otorga permiso para cancelar la actualización de software de servicio de un dominio. Este permiso está obsoleto. Úselo CancelServiceSoftwareUpdate en su lugar	Escritura	domain*		
CancelServiceSoftwareUpdate	Otorga permiso para cancelar la actualización de software de servicio de un dominio	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Otorga permiso para crear una OpenSearch aplicación	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Otorga permiso para crear un dominio OpenSearch de Amazon Service	Escritura	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchDomain	Otorga permiso para crear un dominio OpenSearch de servicio. Este permiso está obsoleto. Úselo CreateDomain en su lugar	Escritura	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchServiceRole	Otorga permiso para crear el rol vinculado al servicio necesario para los dominios de OpenSearch servicio que utilizan el acceso a la VPC. Este permiso está obsoleto. OpenSearch El servicio crea el rol vinculado al servicio por usted	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateOutboundConnection	Otorga permiso para crear una nueva conexión de búsqueda entre clústeres desde un dominio de origen a un dominio de destino	Escritura	domain*		
CreateOutboundCrossClusterSearchConnection	Otorga permiso para crear una nueva conexión de búsqueda entre clústeres desde un dominio fuente a uno de destino. Este permiso está obsoleto. Úselo en su lugar CreateOutboundConnection	Escritura	domain*		
CreatePackage	Otorga permiso para añadir un paquete para su uso con los dominios OpenSearch de servicio	Escritura			
CreateServiceRole	Otorga permiso para crear el rol vinculado al servicio necesario para los dominios de Amazon OpenSearch Service que utilizan el acceso a la VPC	Escritura			
CreateVpcEndpoint	Otorga permiso para crear un punto final de OpenSearch VPC gestionado por Amazon Service	Escritura			
DeleteApplication	Otorga permiso para eliminar una aplicación OpenSearch	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDataSource	Otorga permiso para eliminar la fuente de datos del dominio del OpenSearch servicio	Escritura	domain*		
DeleteDirectQueryDataSource	Otorga permiso para eliminar la fuente de datos de los OpenSearch arns proporcionados	Escritura	datasource*		
DeleteDomain	Otorga permiso para eliminar un dominio de Amazon OpenSearch Service y todos sus datos	Escritura	domain*		
DeleteElasticsearchDomain	Otorga permiso para eliminar un dominio de OpenSearch servicio y todos sus datos. Este permiso está obsoleto. Úselo DeleteDomain en su lugar	Escritura	domain*		
DeleteElasticsearchServiceRole	Otorga permiso para eliminar la función vinculada al servicio necesaria para los dominios de OpenSearch servicio que utilizan el acceso a la VPC. Este permiso está obsoleto. Utilice la API de IAM para eliminar roles vinculados a servicios	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteInboundConnection	Otorga permiso al propietario del dominio de destino para eliminar una conexión de búsqueda entre clústeres entrantes existentes	Escritura			
DeleteInboundCrossClusterSearchConnection	Otorga permiso al propietario del dominio de destino para eliminar una conexión de búsqueda existente entre clústeres entrantes. Este permiso está obsoleto. DeleteInboundConnection Úselo en su lugar	Escritura			
DeleteOutboundConnection	Otorga permiso al propietario del dominio de origen para eliminar una conexión de búsqueda entre clúster saliente existente	Escritura			
DeleteOutboundCrossClusterSearchConnection	Otorga permiso al propietario del dominio fuente para eliminar una conexión de búsqueda existente entre clústeres salientes. Este permiso está obsoleto. Úselo DeleteOutboundConnection en su lugar	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePackage	Otorga permiso para eliminar un paquete del OpenSearch Servicio. El paquete no debe estar asociado con ningún dominio	Escritura			
DeleteVpcEndpoint	Concede permiso para eliminar un punto final de VPC de OpenSearch interfaz gestionada por Amazon Service	Escritura			
DescribeDomain	Otorga permiso para ver una descripción de la configuración de dominio para el dominio de OpenSearch servicio especificado, incluidos el ID de dominio, el punto final del servicio y el ARN	Lectura	domain*		
DescribeDomainAutoTunes	Otorga permiso para ver la configuración de Auto-Tune del dominio para el dominio de OpenSearch servicio especificado, incluidos los programas de estado y mantenimiento de Auto-Tune	Lectura	domain*		
DescribeDomainChangeProgress	Otorga permiso para ver en detalle el progreso de las etapas de un dominio de servicio OpenSearch	Lectura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDomainConfig	Otorga permiso para ver una descripción de las opciones de configuración y el estado de un dominio de OpenSearch servicio	Lectura	domain*		
DescribeDomainHealth	Otorga permiso para ver información sobre el estado del dominio y del nodo, la zona de disponibilidad en espera, el número de nodos por zona de disponibilidad y el número de partición por nodo	Lectura	domain*		
DescribeDomainNodes	Concede permiso para ver información sobre los nodos configurados para el dominio y sus configuraciones: ID del nodo, tipo de nodo, estado del nodo, zona de disponibilidad, tipo de instancia y almacenamiento	Lectura	domain*		
DescribeDomains	Otorga permiso para ver una descripción de la configuración del dominio para un máximo de cinco dominios de OpenSearch servicio específicos	Enumeración	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDryRunProgress	Otorga permiso para describir el estado de una comprobación de validación previa a la actualización en un dominio OpenSearch de servicio	Lectura	domain*		
DescribeElasticsearchDomain	Otorga permiso para ver una descripción de la configuración de dominio para el dominio de OpenSearch servicio especificado, incluidos el ID de dominio, el punto final del servicio y el ARN. Este permiso está obsoleto. Úselo DescribeDomain en su lugar	Lectura	domain*		
DescribeElasticsearchDomainConfig	Otorga permiso para ver una descripción de la configuración y el estado de un dominio de OpenSearch servicio. Este permiso está obsoleto. Úselo DescribeDomainConfig en su lugar	Lectura	domain*		
DescribeElasticsearchDomains	Otorga permiso para ver una descripción de la configuración del dominio para un máximo de cinco OpenSearch dominios de Amazon específicos. Este permiso está obsoleto. Úselo DescribeDomains en su lugar	Enumeración	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeElasticsearchInstanceTypeLimits	Otorga permiso para ver el número de instancias, el almacenamiento y los límites del nodo maestro para una OpenSearch versión y un tipo de instancia determinados. Este permiso está obsoleto. Úselo DescribeInstanceTypeLimits en su lugar	Enumeración			
DescribeInboundConnections	Otorga permiso con el fin de enumerar todas las conexiones entrantes de búsqueda entre clústeres para un dominio de destino	Enumeración			
DescribeInboundCrossClusterSearchConnections	Otorga permiso con el fin de enumerar todas las conexiones entrantes de búsqueda entre clústeres para un dominio de destino. Este permiso está obsoleto. Úselo DescribeInboundConnections en su lugar	Enumeración			
DescribeInstanceTypeLimits	Otorga permiso para ver los límites del recuento de instancias, el almacenamiento y los nodos maestros para una determinada versión y tipo de instancia del motor	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeOutboundConnections	Otorga permiso con el fin de enumerar todas las conexiones de búsqueda entre clústeres salientes para un dominio de origen	Enumeración			
DescribeOutboundCrossClusterSearchConnections	Otorga permiso con el fin de enumerar todas las conexiones de búsqueda entre clústeres salientes para un dominio fuente. Este permiso está obsoleto. Úselo DescribeOutboundConnections en su lugar	Enumeración			
DescribePackages	Otorga permiso para describir todos los paquetes disponibles para los dominios OpenSearch de servicio	Lectura			
DescribeReservedElasticsearchInstanceOfferings	Otorga permiso para obtener ofertas de instancias reservadas para Amazon OpenSearch Service. Este permiso está obsoleto. Úselo DescribeReservedInstanceOfferings en su lugar	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReservedElasticsearchInstances	Otorga permiso para buscar instancias reservadas de OpenSearch servicio que ya se hayan comprado. Este permiso está obsoleto. Úselo DescribeReservedInstances en su lugar	Enumeración			
DescribeReservedInstanceOfferings	Otorga permiso para obtener ofertas de instancias reservadas para el servicio OpenSearch	Enumeración			
DescribeReservedInstances	Otorga permiso para recuperar instancias reservadas de OpenSearch servicio que ya se hayan comprado	Enumeración			
DescribeVpcEndpoints	Otorga permiso para describir uno o más puntos de enlace de OpenSearch VPC gestionados por Amazon Service	Enumeración			
DissociatePackage	Otorga permiso para desasociar un paquete del dominio de servicio especificado OpenSearch	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DissociatePackages	Otorga permiso para desasociar varios paquetes del dominio de servicio especificado OpenSearch	Escritura	domain*		
ESCrossClusterGet	Otorga permiso para enviar solicitudes entre clústeres a un dominio de destino	Lectura	domain		
ESHttpDelete	Otorga permiso para enviar solicitudes HTTP DELETE al OpenSearch APIs	Escritura	domain		
ESHttpGet	Otorga permiso para enviar solicitudes HTTP GET al OpenSearch APIs	Lectura	domain		
ESHttpHead	Otorga permiso para enviar solicitudes HTTP HEAD al OpenSearch APIs	Lectura	domain		
ESHttpPatch	Otorga permiso para enviar solicitudes HTTP PATCH al OpenSearch APIs	Escritura	domain		
ESHttpPost	Otorga permiso para enviar solicitudes HTTP POST al OpenSearch APIs	Escritura	domain		
ESHttpPut	Otorga permiso para enviar solicitudes HTTP PUT al OpenSearch APIs	Escritura	domain		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetApplication	Otorga permiso para obtener información sobre una OpenSearch aplicación	Lectura	application*		
GetCompatibleElasticsearchVersions	Otorga permiso para obtener una lista de versiones compatibles OpenSearch y de Elasticsearch a las que se puede actualizar un dominio OpenSearch de servicio. Este permiso está obsoleto. GetCompatibleVersions Úselo en su lugar	Enumeración	domain*		
GetCompatibleVersions	Otorga permiso para obtener una lista de versiones de motores compatibles a las que se puede OpenSearch actualizar un dominio de servicio	Enumeración	domain*		
GetDataSource	Otorga permiso para obtener la fuente de datos del dominio del OpenSearch servicio	Lectura	domain*		
GetDirectQueryDataSource	Otorga permiso para obtener la fuente de datos de los OpenSearch arns proporcionados	Lectura	datasource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDomainMaintenanceStatus	Concede permiso para recuperar el estado de la acción de mantenimiento del nodo	Lectura	domain*		
GetPackageVersionHistory	Concede permiso para recuperar el historial de versiones de un paquete	Lectura			
GetUpgradeHistory	Otorga permiso para obtener el historial de actualizaciones de un dominio de servicio determinado OpenSearch	Lectura	domain*		
GetUpgradeStatus	Otorga permiso para obtener el estado de actualización de un dominio de servicio determinado OpenSearch	Lectura	domain*		
ListApplications	Otorga permiso para enumerar aplicaciones OpenSearch	Enumeración	application*		
ListDataSources	Otorga permiso para recuperar una lista de fuentes de datos para el dominio del OpenSearch servicio	Enumeración	domain*		
ListDirectQueryDataSources	Otorga permiso para recuperar una lista de fuentes de datos para los OpenSearch arns proporcionados	Enumeración	datasource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDomainMaintenances	Otorga permiso para recuperar una lista de acciones de mantenimiento para el dominio del OpenSearch servicio	Enumeración	domain*		
ListDomainNames	Otorga permiso para mostrar los nombres de todos los dominios de OpenSearch servicio que pertenecen al usuario actual	Enumeración			
ListDomainsForPackage	Otorga permiso para enumerar todos los dominios de OpenSearch servicio a los que está asociado un paquete	Enumeración			
ListElasticsearchInstanceTypeDetails	Otorga permiso para enumerar todos los tipos de instancias y las funciones disponibles para una OpenSearch versión determinada. Este permiso está obsoleto. Úselo ListInstanceTypeDetails en su lugar	Enumeración			
ListElasticsearchInstanceTypes	Otorga permiso para enumerar todos los tipos de EC2 instancias compatibles con una OpenSearch versión determinada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListElasticsearchVersions	Otorga permiso para publicar todas OpenSearch las versiones compatibles en Amazon OpenSearch Service. Este permiso está obsoleto. Úselo ListVersions en su lugar	Enumeración			
ListInstanceTypeDetails	Otorga permiso para enumerar todos los tipos de instancias y las funciones disponibles para una versión determinada OpenSearch o para una versión de Elasticsearch	Enumeración			
ListPackagesForDomain	Otorga permiso para enumerar todos los paquetes asociados al dominio del servicio OpenSearch	Enumeración	domain*		
ListScheduledActions	Otorga permiso para recuperar una lista de los cambios de configuración programados para un dominio OpenSearch de servicio	Enumeración	domain*		
ListTags	Otorga permiso para mostrar todas las etiquetas de recursos de un dominio de OpenSearch servicio, fuente de datos o aplicación	Lectura	application*		
			datasource*		
			domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListVersions	Otorga permiso para publicar todas las versiones compatibles OpenSearch y de Elasticsearch en Amazon Service OpenSearch	Enumeración			
ListVpcEndpointAccess	Otorga permiso para recuperar información sobre cada AWS principal al que se le permite acceder a un dominio de Amazon OpenSearch Service determinado mediante el uso de un punto de enlace de VPC de interfaz	Enumeración			
ListVpcEndpoints	Otorga permiso para recuperar todos los puntos de enlace de OpenSearch VPC gestionados por Amazon Service en la región y en la actual Cuenta de AWS	Enumeración			
ListVpcEndpointsForDomain	Otorga permiso para recuperar todos los puntos de enlace de OpenSearch VPC gestionados por Amazon Service asociados a un dominio concreto	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PurchaseReservedElasticsearchInstanceOffering	Otorga permiso para comprar instancias reservadas de servicio. OpenSearch Este permiso está obsoleto. Úselo PurchaseReservedInstanceOffering en su lugar	Escritura			
PurchaseReservedInstanceOffering	Otorga permiso para comprar instancias OpenSearch reservadas	Escritura			
RejectInboundConnection	Otorga permiso al propietario del dominio de destino para rechazar una solicitud de conexión de búsqueda entre clústeres entrantes	Escritura			
RejectInboundCrossClusterSearchConnection	Otorga permiso al propietario del dominio de destino para rechazar una solicitud de conexión de búsqueda entrante entre clústeres. Este permiso está obsoleto. Úselo RejectInboundConnection en su lugar	Escritura			
RemoveTags	Otorga permiso para eliminar etiquetas de recursos de un dominio de OpenSearch servicio, fuente de datos o aplicación	Etiquetado	application*		
			datasource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			domain*		
				aws:TagKeys	
RevokeVpcEndpointAccess	Otorga permiso para revocar el acceso a un dominio de Amazon OpenSearch Service que se proporcionó a través de un punto de enlace de VPC de interfaz	Escritura			
StartDomainMaintenance	Concede permiso para iniciar el mantenimiento en el nodo	Escritura	domain*		
StartElasticsearchServiceSoftwareUpdate	Otorga permiso para comenzar la actualización de software de servicio de un dominio. Este permiso está obsoleto. Úselo en su lugar StartServiceSoftwareUpdate	Escritura	domain*		
StartServiceSoftwareUpdate	Otorga permiso para comenzar la actualización de software de servicio de un dominio	Escritura	domain*		
UpdateApplication	Otorga permiso para actualizar una OpenSearch aplicación	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDataSource	Otorga permiso para actualizar la fuente de datos del dominio del OpenSearch servicio	Escritura	domain*		
UpdateDirectQueryDataSource	Otorga permiso para actualizar la fuente de datos de los OpenSearch arns proporcionados	Escritura	datasource*		
UpdateDomainConfig	Otorga permiso para modificar la configuración de un dominio de OpenSearch servicio, como el tipo de instancia o el número de instancias	Escritura	domain*		
UpdateElasticsearchDomainConfig	Otorga permiso para modificar la configuración de un dominio de OpenSearch servicio, como el tipo de instancia o el número de instancias. Este permiso está obsoleto. Úselo UpdateDomainConfig en su lugar	Escritura	domain*		
UpdatePackage	Otorga permiso para actualizar un paquete para su uso con los dominios OpenSearch de servicio	Escritura			
UpdatePackageScope	Otorga permiso para actualizar el alcance de un paquete	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateScheduledAction	Otorga permiso para reprogramar un cambio de configuración del dominio de OpenSearch servicio planificado para más adelante	Escritura	domain*		
UpdateVpcEndpoint	Concede permiso para modificar un punto final de VPC de OpenSearch interfaz gestionada por Amazon Service	Escritura			
UpgradeDomain	Otorga permiso para iniciar la actualización de un dominio de OpenSearch servicio a una versión determinada	Escritura	domain*		
UpgradeElasticsearchDomain	Otorga permiso para iniciar la actualización de un dominio de OpenSearch servicio a una versión específica. Este permiso está obsoleto. Úselo UpgradeDomain en su lugar	Escritura	domain*		

Tipos de recursos definidos por Amazon OpenSearch Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:es:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}`	aws:ResourceTag/${TagKey}
es_role	`arn:${Partition}:iam::${Account}:role/aws-service-role/es.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService`	aws:ResourceTag/${TagKey}
opensearchservice_role	`arn:${Partition}:iam::${Account}:role/aws-service-role/opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService`	aws:ResourceTag/${TagKey}
datasource	`arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon OpenSearch Service

Amazon OpenSearch Service define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS OpsWorks

AWS OpsWorks (prefijo de servicio:`opsworks`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS OpsWorks
- Tipos de recursos definidos por AWS OpsWorks
- Claves de condición de AWS OpsWorks

Acciones definidas por AWS OpsWorks

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssignInstance	Otorga permiso para asignar una instancia registrada a una capa	Escritura	stack		
AssignVolume	Otorga permiso para asignar uno de los volúmenes de Amazon EBS registrados de la pila en una instancia especificada	Escritura	stack		
AssociateElasticIp	Otorga permiso para asociar una de las direcciones IP elásticas registrada de la pila con una instancia especificada	Escritura	stack		
AttachElasticLoadBalancer	Otorga permiso para adjuntar un balanceador de carga Elastic Load Balancing a una capa especificada	Escritura	stack		
CloneStack	Otorga permiso para crear un clon de una pila especificada	Escritura	stack		
CreateApp	Otorga permiso para crear una aplicación para una pila especificada	Escritura	stack		
CreateDeployment	Otorga permiso para ejecutar comandos de pila o implementación	Escritura	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInstance	Otorga permiso para crear una instancia en una pila especificada	Escritura	stack		
CreateLayer	Otorga permiso para crear una capa	Escritura	stack		
CreateStack	Otorga permiso para crear una nueva pila	Escritura			
CreateUserProfile	Otorga permiso para crear un nuevo perfil de usuario	Escritura			
DeleteApp	Otorga permiso para eliminar una aplicación específica	Escritura	stack		
DeleteInstance	Otorga permiso para eliminar una instancia específica, lo que termina la instancia de Amazon EC2 asociada	Escritura	stack		
DeleteLayer	Otorga permiso para eliminar una capa específica	Escritura	stack		
DeleteStack	Concede permiso para eliminar una pila específica.	Escritura	stack		
DeleteUserProfile	Otorga permiso para eliminar un perfil de usuario	Escritura			
DeregisterEcsCluster	Otorga permiso para eliminar un perfil de usuario	Escritura	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterElasticIp	Otorga permiso para anular el registro de una dirección IP elástica especificada	Escritura	stack		
DeregisterInstance	Otorga permiso para anular el registro de una instancia local EC2 o de Amazon registrada	Escritura	stack		
DeregisterRdsDbInstance	Otorga permiso para anular el registro de una instancia de Amazon RDS	Escritura	stack		
DeregisterVolume	Otorga permiso para anular el registro de un volumen de Amazon EBS	Escritura	stack		
DescribeAgentVersions	Otorga permiso para describir las versiones de los agentes disponibles AWS OpsWorks	Enumeración	stack		
DescribeApps	Otorga permiso para solicitar una descripción del conjunto de aplicaciones especificado	Enumeración	stack		
DescribeCommands	Otorga permiso para describir los resultados de comandos especificados	Enumeración	stack		
DescribeDeployments	Otorga permiso para solicitar una descripción de un conjunto especificado de implementaciones	Enumeración	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEcsClusters	Otorga permiso para describir los clústeres de Amazon ECS que están registrados con una pila	Enumeración	stack		
DescribeElasticIps	Concede permiso para describir direcciones IP elásticas	Enumeración	stack		
DescribeElasticLoadBalancers	Otorga permiso para describir instancias de Elastic Load Balancing de una pila	Enumeración	stack		
DescribeInstances	Otorga permiso para solicitar una descripción de un conjunto de instancias	Enumeración	stack		
DescribeLayers	Otorga permiso para solicitar una descripción de una o más capas en una pila especificada	Enumeración	stack		
DescribeLoadBasedAutoScaling	Otorga permiso para describir configuraciones de Auto Scaling basadas en cargas de capas especificadas	Enumeración	stack		
DescribeMyUserProfile	Otorga permiso para describir la información SSH del usuario	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeOperatingSystems	Otorga permiso para describir los sistemas operativos compatibles con AWS OpsWorks Stacks	Enumeración			
DescribePermissions	Otorga permiso para describir permisos para una pila especificada	Enumeración	stack		
DescribeRaidArrays	Otorga permiso para describir matrices RAID de una instancia	Enumeración	stack		
DescribeRdsDbInstances	Otorga permiso para describir instancias de Amazon RDS.	Enumeración	stack		
DescribeServiceErrors	Otorga permiso para describir los errores AWS OpsWorks del servicio	Enumeración	stack		
DescribeStackProvisioningParameters	Otorga permiso para solicitar una descripción de parámetros de aprovisionamiento de una pila	Enumeración	stack		
DescribeStackSummary	Otorga permiso para describir el número de capas y aplicaciones en una pila especificada y el número de instancias en cada estado, como running_setup u online	Enumeración	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeStacks	Otorga permiso para solicitar una descripción de una o más pilas	Enumeración	stack		
DescribeTimeBasedAutoScaling	Otorga permiso para describir configuraciones de escalado automático basado en tiempo para instancias especificadas	Enumeración	stack		
DescribeUserProfiles	Otorga permiso para describir usuarios especificados	Enumeración			
DescribeVolumes	Otorga permiso para describir volúmenes de Amazon EBS de una instancia	Enumeración	stack		
DetachElasticLoadBalancer	Otorga permiso para separar una instancia de Elastic Load Balancing especificada de su capa	Escritura	stack		
DisassociateElasticIp	Otorga permiso para anular la asociación de una dirección IP elástica de una instancia	Escritura	stack		
GetHostnameSuggestion	Otorga permiso para obtener un nombre de host generado para la capa especificada según el tema de nombre de host actual	Lectura	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GrantAccess	Otorga permiso para conceder el acceso de RDP a una instancia de Windows para un periodo especificado	Escritura	stack		
ListTags	Otorga permiso para devolver una lista de etiquetas que se aplica a una capa o pila especificadas	Enumeración	stack		
RebootInstance	Otorga permiso para reiniciar una instancia especificada	Escritura	stack		
RegisterEcsCluster	Otorga permiso para registrar un clúster de Amazon ECS especificado con una pila	Escritura	stack		
RegisterElasticIp	Otorga permiso para registrar una dirección IP elástica con una pila especificada	Escritura	stack		
RegisterInstance	Otorga permiso para registrar instancias con una pila específica que se crearon fuera de AWS OpsWorks	Escritura	stack		
RegisterRdsDbInstance	Otorga permiso para registrar una instancia de Amazon RDS con una pila	Escritura	stack		
RegisterVolume	Otorga permiso para registrar un volumen de Amazon EBS con una pila especificada	Escritura	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetLoadBasedAutoScaling	Otorga permiso para especificar la configuración de escalado automático basado en la carga para una capa especificada	Escritura	stack		
SetPermission	Otorga permiso para especificar permisos del usuario	Administración de permisos	stack		
SetTimeBasedAutoScaling	Otorga permiso para especificar la configuración de escalado automático basado en el tiempo para una instancia especificada	Escritura	stack		
StartInstance	Otorga permiso para iniciar una instancia especificada	Escritura	stack		
StartStack	Otorga permiso para iniciar instancias de una pila	Escritura	stack		
StopInstance	Otorga permiso para detener una instancia especificada	Escritura	stack		
StopStack	Otorga permiso para detener una pila específica	Escritura	stack		
TagResource	Otorga permiso para aplicar etiquetas a una pila o capa especificada	Etiquetado	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UnassignInstance	Otorga permiso para anular la asignación de una instancia registrada de todas las capas	Escritura	stack		
UnassignVolume	Otorga permiso para anular la asignación de un volumen de Amazon EBS asignado	Escritura	stack		
UntagResource	Otorga permiso para eliminar etiquetas de una pila o capa especificada	Etiquetado	stack		
UpdateApp	Otorga permiso para actualizar una aplicación específica	Escritura	stack		
UpdateElasticIp	Otorga permiso para actualizar un nombre de dirección IP elástica registrada	Escritura	stack		
UpdateInstance	Otorga permiso para actualizar una instancia específica	Escritura	stack		
UpdateLayer	Otorga permiso para actualizar una capa específica	Escritura	stack		
UpdateMyUserProfile	Otorga permiso para actualizar una clave pública SSH a un usuario	Escritura			
UpdateRdsDbInstance	Otorga permiso para actualizar una instancia de Amazon RDS	Escritura	stack		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateStack	Otorga permiso para actualizar una pila específica	Escritura	stack		
UpdateUserProfile	Otorga permiso para actualizar el perfil de usuario especificado	Administración de permisos			
UpdateVolume	Otorga permiso para actualizar el nombre o el punto de montaje de volumen de Amazon EBS	Escritura	stack		

Tipos de recursos definidos por AWS OpsWorks

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

Claves de condición de AWS OpsWorks

OpsWorks no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones para la administración AWS OpsWorks de la configuración

AWS OpsWorks La gestión de la configuración (prefijo de servicio:`opsworks-cm`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la administración de la configuración AWS OpsWorks
- Tipos de recursos definidos por AWS OpsWorks Configuration Management
- Claves de condición para la gestión AWS OpsWorks de la configuración

Acciones definidas por la administración de la configuración AWS OpsWorks

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate Node	Otorga permiso para asociar un nodo a un servidor de administración de configuración	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBackup	Otorga permiso con el fin de crear una copia de seguridad para el servidor especificado	Write			
CreateServer	Otorga permiso para crear un nuevo servidor	Write			
DeleteBackup	Otorga permiso para eliminar la copia de seguridad especificada y posiblemente el bucket de S3	Escritura			
DeleteServer	Otorga permiso para eliminar el servidor especificado con su CloudFormation pila correspondiente y, posiblemente, el bucket de S3	Escritura			
DescribeAccountAttributes	Otorga permiso con el fin de describir los límites de servicio para la cuenta del usuario	List			
DescribeBackups	Otorga permiso con el fin de describir una única copia de seguridad, todas las copias de seguridad de un servidor especificado o todas las copias de seguridad de la cuenta del usuario.	List			
DescribeEvents	Otorga permiso para describir todos los eventos del servidor especificado	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeNodeAssociationStatus	Otorga permiso con el fin de describir el estado de asociación para el token de nodo especificado y el servidor especificado	List			
DescribeServers	Otorga permiso para describir el servidor especificado o todos los servidores de la cuenta del usuario	List			
DisassociateNode	Otorga permiso para desasociar un nodo especificado de un servidor	Write			
ExportServerEngineAttribute	Otorga permiso para exportar un atributo de motor desde un servidor	Read			
ListTagsForResource	Otorga permiso para enumerar las etiquetas que se aplican al servidor especificado o a la copia de seguridad	Read			
RestoreServer	Otorga permiso para aplicar una copia de seguridad al servidor especificado. Posiblemente intercambia la instancia ec2 si se especifica	Write			
StartMaintenance	Otorga permiso para iniciar el mantenimiento del servidor inmediatamente	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para aplicar etiquetas al servidor o copia de seguridad especificados	Etiquetado			
UntagResource	Otorga permiso para eliminar etiquetas del servidor o copia de seguridad especificados	Etiquetado			
UpdateServer	Otorga permiso para actualizar la configuración general del servidor	Write			
UpdateServerEngineAttributes	Otorga permiso con el fin de actualizar la configuración del servidor específica para el tipo de administración de la configuración	Escritura			

Tipos de recursos definidos por AWS OpsWorks Configuration Management

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
server	`arn:${Partition}:opsworks-cm::${Account}:server/${ServerName}/${UniqueId}`	
backup	`arn:${Partition}:opsworks-cm::${Account}:backup/${ServerName}-{Date-and-Time-Stamp-of-Backup}`	

Claves de condición para la gestión AWS OpsWorks de la configuración

OpsworksCM no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Acciones, recursos y claves de condición para AWS Organizations

AWS Organizations (prefijo de servicio:`organizations`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Organizations
- Tipos de recursos definidos por AWS Organizations
- Claves de condición para AWS Organizations

Acciones definidas por AWS Organizations

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptHandshake	Concede permiso para enviar una respuesta al creador de un protocolo de transferencia acepando la acción propuesta por la solicitud de protocolo de transferencia	Escritura	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	Concede permiso para adjuntar una política a una raíz, una unidad organizativa o una cuenta individual	Escritura	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
CancelHandshake	Concede permiso para cancelar un protocolo de transferencia	Escritura	handshake*		
CloseAccount	Otorga permiso para cerrar una organización Cuenta de AWS que ahora forma parte de una organización, ya sea creada dentro de la organización o invitada a unirse a ella	Escritura	account*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccount	Otorga permiso para crear una Cuenta de AWS que sea automáticamente miembro de la organización con las credenciales que realizó la solicitud	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateGovCloudAccount	Otorga permiso para crear una cuenta AWS GovCloud (estadounidense)	Escritura		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateOrganization	Da permiso para crear una organización. La cuenta con las credenciales que llama a la CreateOrganization operación se convierte automáticamente en la cuenta de administración de la nueva organización	Escritura			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	Concede permiso para crear una unidad organizativa (UO) dentro de una raíz o UO principal	Escritura	organizationalunit root		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	Otorga permiso para crear una política que puedes adjuntar a una raíz, a una unidad organizativa (OU) o a una persona Cuenta de AWS	Escritura		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeclineHandshake	Da permiso para rechazar una solicitud de protocolo de enlace. Esto establece el estado del protocolo de transferencia en DECLINED (RECHAZADO) y desactiva la solicitud	Escritura	handshake*		
DeleteOrganization	Concede permiso para eliminar la organización	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteOrganizationalUnit	Concede permiso para eliminar una unidad organizativa desde la raíz u otra UO	Escritura	organizationalunit*		
DeletePolicy	Concede permiso para eliminar una política de su organización	Escritura	policy*		
				organizations:PolicyType	
DeleteResourcePolicy	Otorga permiso para eliminar una política de recursos de su organización	Escritura			
DeregisterDelegatedAdministrator	Otorga permiso para anular el registro del miembro especificado Cuenta de AWS como administrador delegado del AWS servicio especificado por ServicePrincipal	Escritura	account*		
				organizations:ServicePrincipal	
DescribeAccount	Concede permiso para recuperar detalles relacionados con las organizaciones de la cuenta especificada	Lectura	account*		
DescribeCreateAccountStatus	Concede permiso para recuperar el estado actual de una solicitud asincrónica para crear una cuenta	Lectura			
DescribeEffectivePolicy	Concede permiso para recuperar la política efectiva de una cuenta	Lectura	account*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				organizations:PolicyType	
DescribeHandshake	Concede permiso para recuperar información sobre un protocolo de transferencia previamente solicitado	Lectura	handshake*		
DescribeOrganization	Otorga permiso para recuperar detalles sobre la organización a la que pertenecen las credenciales de llamada	Lectura			
DescribeOrganizationalUnit	Concede permiso para recuperar información sobre una unidad organizativa (UO)	Lectura	organizationalunit*		
DescribePolicy	Otorga permiso para recuperar detalles sobre una política	Lectura	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Otorga permiso para recuperar información sobre una política de recursos	Lectura			
DetachPolicy	Concede permiso para desconectar una política de una raíz, una unidad organizativa o una cuenta	Escritura	policy*		
			account		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	Otorga permiso para deshabilitar la integración de un AWS servicio (el servicio especificado por ServicePrincipal) con AWS Organizations	Escritura		organizations:ServicePrincipal	
DisablePolicyType	Concede permiso para desactivar un tipo de política de organización en una raíz	Escritura	root*		
				organizations:PolicyType	
EnableAWSServiceAccess	Otorga permiso para habilitar la integración de un AWS servicio (el servicio especificado por ServicePrincipal) con AWS Organizations	Escritura		organizations:ServicePrincipal	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableAllFeatures	Concede permiso para iniciar el proceso para habilitar todas las características de una organización, mejorándola para que no sólo soporte las características de la Facturación consolidada	Escritura			
EnablePolicyType	Concede permiso para habilitar un tipo de política en una raíz	Escritura	root*		
				organizations:PolicyType	
InviteAccountToOrganization	Otorga permiso para enviar una invitación a otra Cuenta de AWS persona pidiéndole que se una a su organización como cuenta de miembro	Escritura	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
LeaveOrganization	Concede permiso para remover una cuenta de miembro de su organización principal	Escritura			
ListAWSServiceAccessForOrganization	Otorga permiso para recuperar la lista de los AWS servicios para los que ha activado la integración con su organización	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAccounts	Otorga permiso para enumerar todas las cuentas de la organización	Enumeración			
ListAccountsForParent	Concede permiso para obtener una lista de las cuentas de una organización que se encuentran en una raíz o unidad organizativa (UO)	Enumeración	organizationalunit		
			root		
ListChildren	Otorga permiso para enumerar todas las cuentas OUs o cuentas que se encuentran en una unidad organizativa principal o raíz	Enumeración	organizationalunit		
			root		
ListCreateAccountStatus	Concede permiso para obtener una lista de las solicitudes de creación de cuentas asincrónicas de las que actualmente se lleva un seguimiento para la organización	Enumeración			
ListDelegatedAdministrators	Otorga permiso para incluir en la lista las AWS cuentas designadas como administradores delegados en esta organización	Enumeración		organizations:ServicePrincipal	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDelegatedServicesForAccount	Otorga permiso para enumerar los AWS servicios para los que la cuenta especificada es administradora delegada en esta organización	Enumeración	account*		
ListHandshakesForAccount	Concede permiso para obtener una lista de todos los protocolos de transferencia que están asociados con una cuenta	Enumeración			
ListHandshakesForOrganization	Concede permiso para obtener una lista de los protocolos de transferencia que están asociados con la organización	Enumeración			
ListOrganizationalUnitsForParent	Otorga permiso para enumerar todas las unidades organizativas (OUs) de una unidad organizativa principal o raíz	Enumeración	organizationalunit root		
ListParents	Otorga permiso para incluir en la lista las unidades organizativas o raíz (OUs) que actúan como matrices inmediatas de una organización organizativa o cuenta secundaria	Enumeración	account organizationalunit		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPolicies	Concede permiso para ver una lista de todas las políticas de una organización	Enumeración		organizations:PolicyType	
ListPoliciesForTarget	Concede permiso para mostrar todas las políticas que están adjuntadas directamente a una raíz, unidad organizativa (UO) o cuenta	Enumeración	account		
			organizationalunit		
			root		
				organizations:PolicyType	
ListRoots	Concede permiso para obtener una lista de todas las raíces que están definidos en la organización	Enumeración			
ListTagsForResource	Concede permiso para obtener una lista de todas las etiquetas del recurso especificado	Enumeración	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTargetsForPolicy	Otorga permiso para enumerar todas las OUs raíces y cuentas a las que está asociada una política	Enumeración	policy*		
				organizations:PolicyType	
MoveAccount	Concede permiso para mover una cuenta desde su raíz u UO actual a otra raíz o UO principal	Escritura	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	Concede permiso para crear o actualizar una política de recursos.	Escritura	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDelegatedAdministrator	Otorga permiso para registrar la cuenta de miembro especificada a fin de administrar las funciones del AWS servicio de la Organización especificadas por ServicePrincipal	Escritura	account*		
				organizations:ServicePrincipal	
RemoveAccountFromOrganization	Otorga permiso para eliminar la cuenta especificada de la organización	Escritura	account*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar una o más etiquetas al recurso especificado.	Etiquetado	account		
			organizationalunit		
			policy	organizations:PolicyType	
			resourcepolicy		
			root		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una o más etiquetas del recurso especificado.	Etiquetado	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateOrganizationalUnit	Concede permiso para cambiar el nombre de una unidad organizativa (UO)	Escritura	organizationalunit*		
UpdatePolicy	Concede permiso para actualizar una política existente con un nuevo nombre, descripción o contenido	Escritura	policy*		
				organizations:PolicyType	

Tipos de recursos definidos por AWS Organizations

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
account	`arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}`	aws:ResourceTag/${TagKey}
handshake	`arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	

Tipos de recurso	ARN	Claves de condición
organization	arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}	
organizationalunit	arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}	aws:ResourceTag/${TagKey}
resourcepolicy	arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}	aws:ResourceTag/${TagKey}
awspolicy	arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}	
root	arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Organizations

AWS Organizations define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
organizations:PolicyType	Filtra el acceso según el tipo de política especificada	Cadena
organizations:ServicePrincipal	Filtra el acceso por los nombres principales de servicio especificados	Cadena

Acciones, recursos y claves de condición para AWS Outposts

AWS Outposts (prefijo de servicio:`outposts`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Outposts
- Tipos de recursos definidos por AWS Outposts
- Claves de condición para AWS Outposts

Acciones definidas por AWS Outposts

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelCapacityTask	Otorga permiso para cancelar una tarea de capacidad	Escritura	outpost*		
CancelOrder	Concede permiso para cancelar un pedido	Escritura			
CreateOrder	Concede permiso para crear un pedido	Escritura	outpost*		
CreateOutpost	Concede permiso para crear un Outpost	Escritura	site*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivateConnectivityConfig	Concede permiso para crear una configuración de conectividad privada	Escritura	outpost*		
CreateSite	Concede permiso para crear un sitio	Escritura		aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteOutpost	Concede permiso para eliminar un Outpost	Escritura	outpost*		
DeleteSite	Concede permiso para eliminar un sitio	Escritura	site*		
GetCapacityTask	Otorga permiso para obtener información sobre la tarea de capacidad especificada	Lectura	outpost*		
GetCatalogItem	Concede permiso para obtener un elemento de catálogo	Lectura			
GetConnection	Concede permiso para obtener información acerca de las configuraciones de su servidor de Outpost	Lectura			
GetOrder	Concede permiso para obtener información sobre una orden	Lectura			
GetOutpost	Concede permiso para obtener información acerca del Outpost especificado	Lectura	outpost*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOutpostInstanceTypes	Concede permiso para obtener los tipos de instancia para el Outpost especificado	Lectura	outpost*		
GetOutpostSupportedInstanceTypes	Concede permiso para obtener los tipos de instancia admitidos para el Outpost especificado	Lectura	outpost*		
GetPrivateConnectivityConfig	Concede permiso para obtener una configuración de conectividad privada	Lectura	outpost*		
GetSite	Concede permiso para obtener un sitio	Lectura	site*		
GetSiteAddress	Concede permiso para obtener la dirección de un sitio	Lectura	site*		
ListAssetInstances	Otorga permiso para enumerar todas las instancias en ejecución del Outpost especificado	Enumeración	outpost*		
ListAssets	Concede permiso para enumerar los activos de su Outpost	Enumeración	outpost*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBlockingInstancesForCapacityTask	Otorga permiso para enumerar todas las instancias en ejecución que bloquean la ejecución de la tarea de capacidad para el Outpost especificado	Enumeración	outpost*		
ListCapacityTasks	Otorga permiso para enumerar las tareas de capacidad de su Cuenta de AWS	Enumeración			
ListCatalogItems	Concede permiso para enumerar todos los elementos de catálogo	Enumeración			
ListOrders	Otorga permiso para publicar los pedidos de su Cuenta de AWS	Enumeración			
ListOutposts	Otorga permiso para publicar los Outposts para tu Cuenta de AWS	Enumeración			
ListSites	Otorga permiso para publicar los sitios para su Cuenta de AWS	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCapacityTask	Otorga permiso para crear una tarea de capacidad	Escritura	outpost*		
StartConnection	Concede permiso para iniciar una conexión para su servidor de Outpost	Escritura			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	outpost		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	outpost		
			site		
				aws:TagKeys	
UpdateOutpost	Concede permiso para actualizar un Outpost	Escritura	outpost*		
UpdateSite	Concede permiso para actualizar un sitio	Escritura	site*		
UpdateSiteAddress	Concede permiso para actualizar la dirección del sitio	Escritura	site*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSiteRackPhysicalProperties	Concede permiso para actualizar las propiedades físicas de un bastidor de un sitio	Escritura	site*		

Tipos de recursos definidos por AWS Outposts

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Outposts

AWS Outposts define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Panorama

AWS Panorama (prefijo de servicio:`panorama`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Panorama
- Tipos de recursos definidos por AWS Panorama
- Claves de condición para AWS Panorama

Acciones definidas por AWS Panorama

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplicationInstance	Otorga permiso para crear una instancia de aplicación AWS Panorama	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateJobForDevices	Otorga permiso para crear un trabajo para un dispositivo AWS Panorama	Escritura			
CreateNodeFromTemplateJob	Otorga permiso para crear un nodo AWS Panorámico	Escritura			
CreatePackage	Otorga permiso para crear un Paquete AWS Panorama	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePackageImportJob	Otorga permiso para crear un Paquete AWS Panorama	Escritura			
DeleteDevice	Otorga permiso para anular el registro de un dispositivo Panorama AWS	Escritura	device*		
DeletePackage	Otorga permiso para eliminar un Paquete AWS Panorama	Escritura	package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterPackageVersion	Otorga permiso para anular el registro de una versión del paquete AWS Panorama	Escritura	package*		
DescribeApplicationInstance	Otorga permiso para ver los detalles de una instancia de la aplicación AWS Panorama	Lectura	applicationInstance*		
DescribeApplicationInstanceDetails	Otorga permiso para ver los detalles de una instancia de la aplicación AWS Panorama	Lectura	applicationInstance*		
DescribeDevice	Otorga permiso para ver los detalles de un dispositivo AWS Panorama	Lectura	device*		
DescribeDeviceJob	Otorga permiso para ver los detalles del trabajo de un dispositivo AWS Panorama	Lectura			
DescribeNode	Otorga permiso para ver detalles sobre un nodo de la aplicación AWS Panorama	Lectura			
DescribeNodeFromTemplateJob	Otorga permiso para ver detalles sobre el nodo de la aplicación AWS Panorama	Lectura			
DescribePackage	Otorga permiso para ver los detalles de un paquete AWS Panorama	Lectura	package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePackageImportJob	Otorga permiso para ver los detalles de un paquete AWS Panorama	Lectura			
DescribePackageVersion	Otorga permiso para ver los detalles de una versión del paquete AWS Panorama	Lectura	package*		
DescribeSoftware [solo permiso]	Otorga permiso para ver detalles sobre una versión de software del Dispositivo AWS Panorama	Lectura			
GetWebSocketURL [solo permiso]	Otorga permiso para generar un WebSocket punto final para la comunicación con AWS Panorama	Lectura			
ListApplicationInstanceDependencies	Otorga permiso para recuperar una lista de dependencias de instancias de aplicaciones en Panorama AWS	Enumeración	applicationInstance*		
ListApplicationInstanceNodeInstances	Otorga permiso para recuperar una lista de instancias de nodos de instancias de aplicaciones en AWS Panorama	Enumeración	applicationInstance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApplicationInstances	Otorga permiso para recuperar una lista de instancias de aplicaciones en AWS Panorama	Enumeración	device		
ListDevices	Otorga permiso para recuperar una lista de dispositivos en AWS Panorama	Enumeración			
ListDevicesJobs	Otorga permiso para recuperar una lista de trabajos para un dispositivo AWS Panorama	Enumeración	device		
ListNodeFromTemplateJobs	Concede permiso para recuperar una lista de nodos para un dispositivo AWS Panorama	Enumeración			
ListNodes	Otorga permiso para recuperar una lista de nodos en AWS Panorama	Enumeración			
ListPackageImportJobs	Otorga permiso para recuperar una lista de paquetes en AWS Panorama	Enumeración			
ListPackages	Otorga permiso para recuperar una lista de paquetes en AWS Panorama	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para recuperar una lista de etiquetas para un recurso en AWS Panorama	Lectura	applicationInstance		
			device		
			package		
ProvisionDevice	Otorga permiso para registrar un dispositivo AWS Panorama	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterPackageVersion	Otorga permiso para registrar una versión del paquete AWS Panorama	Escritura	package*		
RemoveApplicationInstance	Otorga permiso para eliminar una instancia de la aplicación AWS Panorama	Escritura	applicationInstance*		
SignalApplicationInstanceNodeInstances	Otorga permiso a los nodos de la cámara de señal en una instancia de aplicación para que se detengan o reanuden	Escritura	applicationInstance*		
TagResource	Otorga permiso para añadir etiquetas a un recurso en AWS Panorama	Etiquetado	applicationInstance		
			device		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			package		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso en AWS Panorama	Etiquetado	applicationInstance		
			device		
			package		
				aws:TagKeys	
UpdateDeviceMetadata	Otorga permiso para modificar la configuración básica de un dispositivo AWS Panorama	Escritura	device*		

Tipos de recursos definidos por AWS Panorama

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
device	`arn:${Partition}:panorama:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}
package	`arn:${Partition}:panorama:${Region}:${Account}:package/${PackageId}`	aws:ResourceTag/${TagKey}
applicationInstance	`arn:${Partition}:panorama:${Region}:${Account}:applicationInstance/${ApplicationInstanceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Panorama

AWS Panorama define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Parallel Computing Service

AWS Parallel Computing Service (prefijo de servicio:`pcs`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Parallel Computing Service
- Tipos de recursos definidos por AWS Parallel Computing Service
- Claves de condición para AWS Parallel Computing Service

Acciones definidas por AWS Parallel Computing Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Otorga permiso para configurar la entrega de registros vendida para los registros del clúster de AWS PCS	Escritura	cluster*		
CreateCluster	Concede permiso para crear clústeres	Escritura		aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole secretsmanager:CreateSecret

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:TagResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateComputeNodeGroup	Concede permiso para crear grupos de nodos de computación	Escritura	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Concede permiso para crear colas	Escritura	cluster*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Concede permiso para eliminar clústeres	Escritura	cluster*		ec2:DeleteNetworkInterface secretsmanager:DeleteSecret

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteComputeNodeGroup	Concede permiso para eliminar grupos de nodos de computación	Escritura	cluster*		ec2:DeleteLaunchTemplate ec2:TerminateInstances
			computenodegroup*		
DeleteQueue	Concede permiso para eliminar colas	Escritura	cluster*		
			queue*		
GetCluster	Concede permiso para obtener las propiedades del clúster	Lectura	cluster*		
GetComputeNodeGroup	Concede permiso para obtener las propiedades del grupo de nodos de computación	Lectura	cluster*		
			computenodegroup*		
GetQueue	Concede permiso para obtener las propiedades de la cola	Lectura	cluster*		
			queue*		
ListClusters	Concede permiso para enumerar clústeres	Enumeración			
ListComputeNodeGroups	Concede permiso para enumerar los grupos de nodos de computación	Enumeración	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQueues	Concede permiso para enumerar colas	Enumeración	cluster*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
RegisterComputeNodeGroupInstance	Concede permiso para registrar una instancia de computación en un grupo de nodos de computación	Escritura	cluster*		secretsmanager:GetSecretValue
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	cluster	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateComputeNodeGroup	Concede permiso para actualizar las propiedades del grupo de nodos de computación	Escritura	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole
			computenodegroup*		
UpdateQueue	Concede permiso para actualizar las propiedades de la cola	Escritura	cluster*		
			queue*		

Tipos de recursos definidos por AWS Parallel Computing Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}`	aws:ResourceTag/${TagKey}
computenodegroup	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/computenodegroup/${ComputeNodeGroupIdentifier}`	aws:ResourceTag/${TagKey}
queue	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/queue/${QueueIdentifier}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Parallel Computing Service

AWS Parallel Computing Service define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para la administración de cuenta central de AWS Partner

AWS La administración central de cuentas de los socios (prefijo de servicio:`partnercentral-account-management`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la administración de cuenta central de AWS Partner
- Tipos de recursos definidos por la administración de cuenta central de AWS Partner
- Claves de condición para la administración de cuenta central de AWS Partner

Acciones definidas por la administración de cuenta central de AWS Partner

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociatePartnerAccount [solo permiso]	Otorga permiso para asociar la cuenta del socio a Cuenta de AWS	Escritura			
AssociatePartnerUser	Concede permiso para asociar un usuario Partner al rol de IAM	Escritura			
DisassociatePartnerUser	Concede permiso para desasociar un usuario Partner al rol de IAM	Escritura			

Tipos de recursos definidos por la administración de cuenta central de AWS Partner

AWS La administración de cuentas centrales de socios no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la administración de cuenta central de AWS Partner, especifique `"Resource": "*"` en su política.

Claves de condición para la administración de cuenta central de AWS Partner

La administración de cuenta central Partner no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de acciones, recursos y condiciones de AWS Partner Central Selling

AWS Partner Central Selling (prefijo de servicio:`partnercentral`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Partner Central Selling AWS
- Tipos de recursos definidos por AWS Partner Central Selling
- Claves de condición de AWS Partner Central Selling

Acciones definidas por Partner Central Selling AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptEngagementInvitation	Otorga permiso para aceptar invitaciones de participación en AWS Partner Central	Escritura	engagement-invitation*		
				partnercentral:Catalog	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssignOpportunity	Otorga permiso para asignar oportunidades en AWS Partner Central	Escritura	Opportunity*		
				partnercentral:Catalog	
AssociateOpportunity	Otorga permiso para asociar Opportunities on AWS Partner Central con otras entidades	Escritura	Opportunity*		
				partnercentral:Catalog partnercentral:RelatedEntityType	
CreateEngagement	Otorga permiso para crear interacciones en Partner Central AWS	Escritura		partnercentral:Catalog	
CreateEngagementInvitation	Otorga permiso para crear invitaciones de participación en Partner Central AWS	Escritura		partnercentral:Catalog	
CreateOpportunity	Otorga permiso para crear nuevas oportunidades en AWS Partner Central	Escritura		partnercentral:Catalog	
CreateResourceSnapshot	Otorga permiso para crear instantáneas de recursos en AWS Partner Central	Escritura	ResourceSnapshot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				partnercentral:Catalog	
CreateResourceSnapshotJob	Otorga permiso para crear trabajos de instantáneas de recursos en AWS Partner Central	Escritura		aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	
DeleteResourceSnapshotJob	Otorga permiso para eliminar trabajos de instantáneas de recursos en AWS Partner Central	Escritura	resource-snapshot-job*		
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
DisassociateOpportunity	Otorga permiso para desvincular Opportunities on AWS Partner Central de otras entidades	Escritura	Opportunity*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				partnercentral:Catalog partnercentral:RelatedEntityType	
GetAwsOpportunitySummary	Otorga permiso para recuperar AWS los resúmenes de las oportunidades en Partner Central AWS	Lectura	Opportunity*		
				partnercentral:Catalog	
GetEngagement	Otorga permiso para recuperar los detalles de la contratación en Partner Central AWS	Lectura	Engagement*		
				partnercentral:Catalog	
GetEngagementInvitation	Otorga permiso para recuperar los detalles de las invitaciones de participación en AWS Partner Central	Lectura	engagement-invitation*		
				partnercentral:Catalog	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOpportunity	Otorga permiso para recuperar los detalles de las oportunidades en AWS Partner Central	Lectura	Opportunity*		
				partnercentral:Catalog	
GetResourceSnapshot	Otorga permiso para recuperar los detalles de la instantánea de los recursos en AWS Partner Central	Lectura	ResourceSnapshot*		
				partnercentral:Catalog	
GetResourceSnapshotJob	Otorga permiso para recuperar los detalles de las tareas instantáneas de los recursos en Partner Central AWS	Lectura	resource-snapshot-job*		
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
GetSellingSystemSettings	Otorga permiso para recuperar la configuración del sistema en Partner Central AWS	Lectura		partnercentral:Catalog	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEngagementByAcceptingInvitationTasks	Otorga permiso para publicar compromisos al aceptar tareas por invitación en Partner Central AWS	Enumeración		partnercentral:Catalog	
ListEngagementFromOpportunityTasks	Otorga permiso para incluir en Partner Central los compromisos de las tareas de oportunidad AWS	Enumeración		partnercentral:Catalog	
ListEngagementInvitations	Otorga permiso para publicar las invitaciones de participación en Partner Central AWS	Enumeración		partnercentral:Catalog	
ListEngagementMembers	Otorga permiso para incluir a los miembros del compromiso en AWS Partner Central	Lectura	Engagement*		
				partnercentral:Catalog	
ListEngagementResourceAssociations	Otorga permiso para incluir asociaciones de recursos de participación en AWS Partner Central	Lectura	ResourceSnapshot*		
				partnercentral:Catalog	
ListEngagements	Otorga permiso para incluir las participaciones en Partner Central AWS	Enumeración		partnercentral:Catalog	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOpportunities	Otorga permiso para publicar oportunidades en Partner Central AWS	Enumeración		partnercentral:Catalog	
ListResourceSnapshotJobs	Otorga permiso para publicar trabajos instantáneos de recursos en AWS Partner Central	Enumeración		partnercentral:Catalog	
ListResourceSnapshots	Otorga permiso para incluir instantáneas de recursos en AWS Partner Central	Lectura	ResourceSnapshot*		
				partnercentral:Catalog	
ListSolutions	Otorga permiso para incluir soluciones en AWS Partner Central	Enumeración		partnercentral:Catalog	
ListTagsForResource	Otorga permiso para añadir etiquetas de listas a un recurso. Recurso compatible: ResourceSnapshotJob	Lectura		aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
PutSellingSystemSettings	Otorga permiso para colocar los ajustes del sistema en AWS Partner Central	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RejectEngagementInvitation	Otorga permiso para rechazar las invitaciones de participación en AWS Partner Central	Escritura	engagement-invitation*		
				partnercentral:Catalog	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartEngagementByAcceptingInvitationTask	Otorga permiso para iniciar tareas que den inicio a las interacciones en AWS Partner Central al aceptar una invitación de participación	Escritura		aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	partnercentral:AcceptEngagementInvitation partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagementInvitation partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartEngagementFromOpportunityTask	Otorga permiso para iniciar tareas que inicien interacciones a partir de oportunidades en Partner Central AWS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	partnercentral:CreateEngagement partnercentral:CreateEngagementInvitation partnercentral:CreateResourceSnapshotJob partnercentral:GetOpportunity partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartResourceSnapshotJob	Otorga permiso para iniciar trabajos de captura de recursos en Partner Central AWS	Escritura	resource-snapshot-job*		
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
StopResourceSnapshotJob	Otorga permiso para detener los trabajos de captura de recursos en AWS Partner Central	Escritura	resource-snapshot-job*		
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
SubmitOpportunity	Otorga permiso para enviar oportunidades en AWS Partner Central	Escritura	Opportunity*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				partnercentral:Catalog	
TagResource	Otorga permiso para añadir nuevas etiquetas a un recurso. Recurso compatible: ResourceSnapshotJob	Etiquetado		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
UntagResource	Concede permiso para eliminar etiquetas de un recurso. Recurso compatible: ResourceSnapshotJob	Etiquetado		aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
UpdateOpportunity	Otorga permiso para actualizar las oportunidades en AWS Partner Central	Escritura	Opportunity*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				partnercentral:Catalog	

Tipos de recursos definidos por AWS Partner Central Selling

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Engagement	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement/${Identifier}`	
engagement-by-accepting-invitation-task	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-by-accepting-invitation-task/${TaskId}`	
engagement-from-opportunity-task	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-from-opportunity-task/${TaskId}`	
engagement-invitation	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-invitation/${Identifier}`	

Tipos de recurso	ARN	Claves de condición
Opportunity	`arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/opportunity/${Identifier}`	
resource-snapshot-job	`arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/resource-snapshot-job/${Identifier}`	
ResourceSnapshot	`arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/engagement/${EngagementIdentifier}/resource/${ResourceType}/${ResourceIdentifier}/template/${TemplateIdentifier}/resource-snapshot/${SnapshotRevision}`	
Solution	`arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/solution/${Identifier}`	

Claves de condición de AWS Partner Central Selling

AWS Partner Central Selling define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
partnercentral:Catalog	Filtra el acceso mediante un catálogo específico. Valores aceptados: [AWS, Sandbox]	Cadena
partnercentral:RelatedEntityType	Filtra el acceso por tipos de entidad para la asociación de oportunidades. Valores aceptados: [Soluciones, AwsProducts, AwsMarketplaceOffers]	Cadena

Acciones, recursos y claves de condición para Criptografía de pagos de AWS

AWS La criptografía de pagos (prefijo de servicio:`payment-cryptography`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Criptografía de pagos de AWS

- Tipos de recursos definidos por Criptografía de pagos de AWS
- Claves de condiciones para Criptografía de pagos de AWS

Acciones definidas por Criptografía de pagos de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAlias	Concede permiso para crear un nombre fácil de usar para una clave	Escritura	alias*		
			key*		
CreateKey	Otorga permiso para crear una clave gestionada por el cliente única en la persona que llama y en la región Cuenta de AWS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
DecryptData	Concede permiso para descifrar datos de texto cifrado en texto plano mediante una clave de cifrado de datos simétrica, asimétrica o DUKPT	Escritura	alias*		
			key*		
DeleteAlias	Concede permiso para eliminar el alias de la especificada	Escritura	alias*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteKey	Concede permiso para programar la eliminación de una clave	Escritura	key*		
EncryptData	Concede permiso para cifrar datos de texto plano y convertirlos en texto cifrado mediante una clave de cifrado de datos simétrica, asimétrica o DUKPT	Escritura	alias*		
			key*		
ExportKey	Concede permiso para exportar una clave del servicio	Escritura	key*		
GenerateCardValidationData	Otorga permiso para generar datos relacionados con las tarjetas mediante algoritmos como los valores de verificación de la tarjeta (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) o los códigos de seguridad de la tarjeta (CSC) que comprueban la validez de una tarjeta con banda magnética	Escritura	alias*		
			key*		
GenerateMac	Concede permiso para generar un criptograma MAC (código de autenticación de mensajes)	Escritura	alias*		
			key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateMacEmvPinChange	Concede permiso para generar un criptograma MAC (código de autenticación de mensajes)	Escritura	alias*		
			key*		
GeneratePinData	Permite generar datos relacionados con el PIN, como el PIN, el valor de verificación del PIN (PVV), el bloqueo del PIN y la compensación del PIN durante la emisión o la reemisión de una nueva tarjeta	Escritura	alias*		
			key*		
GetAlias	Concede permiso para recuperar el keyArn asociado a un aliasName	Lectura	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetKey	Concede permiso para devolver información acerca de la clave especificada	Lectura	key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetParametersForExport	Concede permiso para obtener el token de exportación y el certificado de clave de firma para iniciar una exportación de clave TR-34	Lectura			
GetParametersForImport	Concede permiso para obtener el token de importación y el certificado de clave de encapsulación para iniciar la importación de una clave TR-34	Lectura			
GetPublicKeyCertificate	Concede permiso para devolver la clave pública de una clave de la clase PUBLIC_KEY	Lectura	key*		
ImportKey	Concede permiso para importar claves y certificados de clave pública	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
ListAliases	Otorga permiso para devolver una lista de los alias creados para todas las claves de la persona que llama y de la región Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListKeys	Otorga permiso para devolver una lista de claves creadas en la persona que llama y en la región Cuenta de AWS	Enumeración			
ListTagsForResource	Otorga permiso para devolver una lista de etiquetas creadas en la persona que llama y en la región Cuenta de AWS	Lectura	key		
ReEncryptData	Concede permiso para volver a cifrar el texto cifrado mediante DUKPT y claves de cifrado de datos simétricas y asimétricas	Escritura	alias* key*		
RestoreKey	Concede permiso para cancelar la eliminación programada de una clave si en algún momento del período de espera es necesario reactivar una clave	Escritura	key*		
StartKeyUsage	Concede permiso para habilitar una clave desactivada	Escritura	key*		
StopKeyUsage	Concede permiso para desactivar una clave habilitada	Escritura	key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para agregar o sobrescribir una o varias etiquetas para el recurso especificado	Etiquetado	key*		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
TranslatePinData	Concede permiso para traducir un bloque PIN cifrado desde y hacia los formatos ISO 9564 0,1,3,4	Escritura	alias*		
			key*		
UntagResource	Concede permiso para quitar las etiquetas especificadas de los recursos especificados	Etiquetado	key*		
				aws:TagKeys	
UpdateAlias	Concede permiso para cambiar la clave a la que está asignado un alias o anular la asignación de su clave actual	Escritura	alias*		
			key*		
				aws:RequestTag/${TagKey}	
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
VerifyAuthRequestCryptogram	Concede permiso para verificar el criptograma de solicitud de autorización (ARQC) para la autorización de una tarjeta de pago con chip EMV	Escritura	alias*		
			key*		
VerifyCardValidationData	Otorga permiso para verificar los datos de validación relacionados con las tarjetas mediante algoritmos como los valores de verificación de las tarjetas (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) y los códigos de seguridad de las tarjetas (CSC)	Escritura	alias*		
			key*		
VerifyMac	Concede permiso para verificar el MAC (código de autenticación de mensajes) de los datos de entrada con un MAC proporcionado	Escritura	alias*		
			key*		
VerifyPinData	Concede permiso para verificar los datos relacionados con el PIN, como el PIN y el PIN Offset, mediante algoritmos como VISA PVV y IBM3624	Escritura	alias*		
			key*		

Tipos de recursos definidos por Criptografía de pagos de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
key	`arn:${Partition}:payment-cryptography:${Region}:${Account}:key/${KeyId}`	aws:ResourceTag/${TagKey} payment-cryptography:ResourceAliases
alias	`arn:${Partition}:payment-cryptography:${Region}:${Account}:alias/${Alias}`	payment-cryptography:ResourceAliases

Claves de condiciones para Criptografía de pagos de AWS

AWS La criptografía de pagos define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso tanto por la clave como por el valor de la etiqueta de la solicitud para la operación especificada	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso según las etiquetas asignadas a una clave para la operación especificada	Cadena
aws:TagKeys	Filtra el acceso a las claves de etiqueta en la solicitud para la operación especificada	ArrayOfString
payment-cryptography:CertificateAuthorityPublicKeyIdentifier	Filtra el acceso según lo CertificateAuthorityPublicKeyIdentifier especificado en la solicitud o en ExportKey las operaciones y ImportKey	Cadena
payment-cryptography:ImportKeyMaterial	Filtra el acceso por el tipo de material clave que se importa [RootCertificatePublicKey, TrustedCertificatePublicKey, Tr34KeyBlock, Tr31KeyBlock] para la operación ImportKey	Cadena
payment-cryptography:KeyAlgorithm	Filtra el acceso según lo KeyAlgorithm especificado en la solicitud de la operación CreateKey	Cadena
payment-cryptography:KeyClass	Filtra el acceso según lo KeyClass especificado en la solicitud de la CreateKey operación	Cadena
payment-cryptography:KeyUsage	Filtra el acceso según lo KeyClass especificado en la solicitud o asociado a una clave para la CreateKey operación	Cadena
payment-cryptography:RequestAlias	Filtra el acceso por alias en la solicitud para la operación especificada	Cadena

Claves de condición	Descripción	Tipo
payment-cryptography:ResourceAliases	Filtra el acceso por alias asociados con una clave para la operación especificada	ArrayOfString
payment-cryptography:WrappingKeyIdentifier	Filtra el acceso según lo WrappingKeyIdentifier especificado en la solicitud para ImportKey las ExportKey operaciones y	Cadena

Acciones, recursos y claves de condición para AWS Payments

AWS Payments (prefijo de servicio:`payments`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Payments
- Tipos de recursos definidos por AWS Payments
- Claves de condición para AWS Payments

Acciones definidas por AWS Payments

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptFinancingApplicationTerms	Otorga permiso para aceptar las condiciones de solicitud de financiación proporcionadas por un prestamista	Escritura			
CreateFinancingApplication	Otorga permiso para crear una solicitud de financiación	Escritura			
CreatePaymentInstrument	Concede permiso para crear un instrumento de pago	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeletePaymentInstrument [solo permiso]	Concede permiso para eliminar un instrumento de pago	Escritura			
GetFinancingApplication	Otorga permiso para obtener información sobre una solicitud de financiación	Lectura			
GetFinancingLine	Otorga permiso para obtener información sobre una línea de financiación	Lectura			
GetFinancingLineWithdrawal	Otorga permiso para obtener información sobre la retirada de una línea de financiación	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFinancingOption	Otorga permiso para obtener información sobre una opción de financiación	Lectura			
GetPaymentInstrument	Concede permiso para obtener información acerca de un instrumento de pago	Enumeración	payment-instrument		
GetPaymentStatus [solo permiso]	Concede permiso para obtener el estado de pago de las facturas	Lectura			
ListFinancingApplications	Otorga permiso para incluir los metadatos de las solicitudes de financiación	Enumeración			
ListFinancingLineWithdrawals	Otorga permiso para incluir los metadatos de las retiradas de fondos de líneas de financiación	Enumeración			
ListFinancingLines	Otorga permiso para incluir los metadatos de las líneas de financiación	Enumeración			
ListPaymentInstruments [solo permiso]	Concede permiso para enumerar los metadatos del instrumento de pago	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPaymentPreferences [solo permiso]	Concede permiso para obtener las preferencias de pago (moneda de pago preferida, método de pago preferido, etc.)	Enumeración			
ListPaymentProgramOptions	Otorga permiso para incluir información sobre las opciones de pago	Enumeración			
ListPaymentProgramStatus	Otorga permiso para incluir información sobre la elegibilidad del programa de pago y el estado de la inscripción	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas en un recurso de pago	Enumeración	payment-instrument		
MakePayment [solo permiso]	Concede permiso para realizar un pago, autenticar un pago, verificar un método de pago y generar un documento de solicitud de fondos para Advance Pay (Pago por adelantado)	Escritura			
TagResource	Concede permiso para etiquetar un recurso de pago	Etiquetado	payment-instrument		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para quitar etiquetas de un recurso de pago	Etiquetado	payment-instrument		
				aws:TagKeys	
UpdateFinancingApplication	Otorga permiso para actualizar una solicitud de financiación	Escritura			
UpdatePaymentInstrument [solo permiso]	Concede permiso para actualizar un instrumento de pago	Escritura			
UpdatePaymentPreferences [solo permiso]	Concede permiso para actualizar las preferencias de pago (moneda de pago preferida, método de pago preferido, etc.)	Escritura			

Tipos de recursos definidos por AWS Payments

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
payment-instrument	`arn:${Partition}:payments::${Account}:payment-instrument:${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Payments

AWS Payments define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Performance Insights

AWS Performance Insights (prefijo de servicio:`pi`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Performance Insights
- Tipos de recursos definidos por AWS Performance Insights
- Claves de condición para AWS Performance Insights

Acciones definidas por AWS Performance Insights

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePerformanceAnalysisReport	Otorga permiso para llamar a la CreatePerformanceAnalysisReport API a fin de crear un informe de análisis de rendimiento para una instancia de base de datos específica	Escritura	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePerformanceAnalysisReport	Otorga permiso para llamar a la DeletePerformanceAnalysisReport API a fin de eliminar un informe de análisis de rendimiento de una instancia de base de datos específica	Escritura	perf-reports-resource*		
DescribeDimensionKeys	Otorga permiso para llamar a la DescribeDimensionKeys API a fin de recuperar las N claves de dimensión principales de una métrica durante un período de tiempo específico	Lectura	metric-resource*		
				pi:Dimensions	
GetDimensionKeyDetails	Otorga permiso para llamar a la GetDimensionKeyDetails API para recuperar los atributos del grupo de dimensiones especificado	Lectura	metric-resource*		
				pi:Dimensions	
GetPerformanceAnalysisReport	Otorga permiso para llamar a la GetPerformanceAnalysisReport API para recuperar un informe de análisis de rendimiento de una instancia de base de datos específica	Lectura	perf-reports-resource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourceMetadata	Otorga permiso para llamar a la GetResourceMetadata API a fin de recuperar los metadatos de diferentes funciones	Lectura	metric-resource*		
GetResourceMetrics	Otorga permiso para llamar a la GetResourceMetrics API para recuperar las métricas de IP de un conjunto de fuentes de datos durante un período de tiempo	Lectura	metric-resource*		
				pi:Dimensions	
ListAvailableResourceDimensions	Otorga permiso para llamar a la ListAvailableResourceDimensions API a fin de recuperar las dimensiones que se pueden consultar para cada tipo de métrica especificado en una instancia de base de datos específica	Lectura	metric-resource*		
ListAvailableResourceMetrics	Otorga permiso para llamar a la ListAvailableResourceMetrics API a fin de recuperar métricas de los tipos especificados que se pueden consultar para una instancia de base de datos específica	Lectura	metric-resource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPerformanceAnalysisReports	Otorga permiso para llamar a la ListPerformanceAnalysisReports API a fin de enumerar los informes de análisis de rendimiento de una instancia de base de datos específica	Enumeración	perf-reports-resource*		
ListTagsForResource	Otorga permiso para llamar a la ListTagsForResource API para enumerar las etiquetas de un recurso	Enumeración	perf-reports-resource*		
TagResource	Otorga permiso para llamar a la TagResource API para etiquetar un recurso	Etiquetado	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para llamar a la UntagResource API para eliminar la etiqueta de un recurso	Etiquetado	perf-reports-resource*		
				aws:TagKeys	

Tipos de recursos definidos por AWS Performance Insights

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	
perf-reports-resource	`arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Performance Insights

AWS Performance Insights define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
pi:Dimensions	Filtra el acceso según las dimensiones solicitadas	ArrayOfString

Acciones, recursos y claves de condición para Amazon Personalize

Amazon Personalize (prefijo de servicio: `personalize`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Personalize
- Tipos de recurso definidos por Amazon Personalize
- Claves de condición de Amazon Personalize

Acciones definidas por Amazon Personalize

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBatchInferenceJob	Otorga permiso para crear un trabajo de inferencia por lotes	Escritura	batchInferenceJob*		
CreateBatchSegmentJob	Otorga permiso para crear un trabajo de segmento por lotes.	Escritura	batchSegmentJob*		
CreateCampaign	Otorga permiso para crear una campaña	Escritura	campaign*		
CreateDataDeletionJob	Concede permiso para crear un trabajo de eliminación de datos	Escritura	dataDeletionJob*		
CreateDataInsightsJob	Otorga permiso para crear un trabajo de análisis de datos	Escritura	dataInsightsJob*		
CreateDataset	Concede permiso para crear un conjunto de datos	Escritura	dataset*		
CreateDatasetExportJob	Otorga permiso para crear un trabajo de exportación de conjunto de datos	Escritura	datasetExportJob*		
CreateDatasetGroup	Concede permiso para crear un grupo de conjuntos de datos.	Write	datasetGroup*		
CreateDatasetImportJob	Concede permiso para crear un trabajo de importación de conjuntos de datos	Write	datasetImportJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEventTracker	Otorga permiso para crear un rastreador de eventos	Write	eventTracker*		
CreateFilter	Otorga permiso para crear un filtro	Escritura	filter*		
CreateMetricAttribution	Otorga permiso para crear una atribución de métricas	Escritura	metricAttribution*		
CreateRecommender	Otorga permiso para crear un recomendador.	Escritura	recommender*		
CreateSchema	Otorga permiso para crear un esquema	Write	schema*		
CreateSolution	Otorga permiso para crear una solución	Write	solution*		
CreateSolutionVersion	Otorga permiso para crear una versión de solución	Write	solution*		
DeleteCampaign	Otorga permiso para eliminar una campaña	Write	campaign*		
DeleteDataset	Concede permiso para eliminar un conjunto de datos	Write	dataset*		
DeleteDatasetGroup	Concede permiso para eliminar un grupo de conjuntos de datos	Write	datasetGroup*		
DeleteEventTracker	Otorga permiso para eliminar un rastreador de eventos	Write	eventTracker*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteFilter	Otorga permiso para eliminar un filtro	Escritura	filter*		
DeleteMetricAttribution	Otorga permiso para eliminar una atribución de métricas	Escritura	metricAttribution*		
DeleteRecommender	Otorga permiso para eliminar un recomendador.	Escritura	recommender*		
DeleteSchema	Otorga permiso para eliminar un esquema	Write	schema*		
DeleteSolution	Otorga permiso para eliminar una solución, incluidas todas las versiones de la solución	Write	solution*		
DescribeAlgorithm	Otorga permiso para describir un algoritmo	Read	algorithm*		
DescribeBatchInferenceJob	Otorga permiso para describir un trabajo de inferencia por lotes	Lectura	batchInferenceJob*		
DescribeBatchSegmentJob	Otorga permiso para describir un trabajo de segmento por lote.	Lectura	batchSegmentJob*		
DescribeCampaign	Otorga permiso para describir una campaña	Lectura	campaign*		
DescribeDataDeletionJob	Concede permiso para describir un trabajo de eliminación de datos	Lectura	dataDeletionJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDataInsightsJob	Otorga permiso para describir un trabajo de análisis de datos	Lectura	dataInsightsJob*		
DescribeDataset	Concede permiso para describir un conjunto de datos	Lectura	dataset*		
DescribeDatasetExportJob	Otorga permiso para describir un trabajo de exportación de conjunto de datos	Lectura	datasetExportJob*		
DescribeDatasetGroup	Concede permiso para describir un grupo de conjuntos de datos	Read	datasetGroup*		
DescribeDatasetImportJob	Concede permiso para describir un trabajo de importación de conjuntos de datos	Read	datasetImportJob*		
DescribeEventTracker	Otorga permiso para describir un rastreador de eventos	Read	eventTracker*		
DescribeFeatureTransformation	Otorga permiso para describir una transformación de características	Read	featureTransformation*		
DescribeFilter	Otorga permiso para describir un filtro	Lectura	filter*		
DescribeMetricAttribution	Otorga permiso para describir una atribución de métrica	Lectura	metricAttribution*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRecipe	Otorga permiso para describir una receta	Lectura	recipe*		
DescribeRecommender	Otorga permiso para describir un recomendador.	Lectura	recommender*		
DescribeSchema	Otorga permiso para describir un esquema	Read	schema*		
DescribeSolution	Otorga permiso para describir una solución	Read	solution*		
DescribeSolutionVersion	Otorga permiso para describir una versión de una solución	Lectura	solution*		
GetActionRecommendations	Concede permiso para obtener una lista de acciones recomendadas	Lectura	campaign*		
GetDataInsights	Otorga permiso para obtener un análisis de datos a partir de un trabajo de análisis de datos	Lectura	dataInsightsJob*		
GetPersonalizedRanking	Otorga permiso para obtener una lista reclasificada de recomendaciones	Read	campaign*		
GetRecommendations	Otorga permiso para obtener una lista de recomendaciones de una campaña	Read	campaign*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSolutionMetrics	Otorga permiso para obtener métricas para una versión de solución	Read	solution*		
ListBatchInferenceJobs	Otorga permiso para enumerar trabajos de inferencia por lotes	Enumeración			
ListBatchSegmentJobs	Otorga permiso para enumerar trabajos de segmentos por lotes.	Enumeración			
ListCampaigns	Otorga permiso para enumerar campañas	Enumeración			
ListDataDeletionJobs	Concede permiso para enumerar trabajos de eliminación de datos	Enumeración			
ListDataInsightsJobs	Otorga permiso para enumerar trabajos de análisis de datos	Enumeración			
ListDatasetExportJobs	Otorga permiso para enumerar trabajos de exportación de conjunto de datos	Enumeración			
ListDatasetGroups	Otorga permiso para enumerar grupos de conjuntos de datos	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDatasetImportJobs	Otorga permiso para enumerar trabajos de importación de conjuntos de datos	List			
ListDatasets	Otorga permiso para enumerar conjuntos de datos	List			
ListEventTrackers	Otorga permiso para enumerar los rastreadores de eventos	List			
ListFilters	Otorga permiso para enumerar filtros	Enumeración			
ListMetricAttributionMetrics	Otorga permiso para enumerar las métricas de atribución de métricas	Enumeración			
ListMetricAttributions	Otorga permiso para enumerar las atribuciones de métricas	Enumeración			
ListRecipes	Otorga permiso para enumerar recetas	Enumeración			
ListRecommenders	Otorga permiso para enumerar los recomendadores.	Enumeración			
ListSchemas	Otorga permiso para enumerar esquemas	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSolutionVersions	Otorga permiso para enumerar versiones de una solución	List			
ListSolutions	Otorga permiso para enumerar soluciones	Enumeración			
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	Enumeración			
PutActionInteractions	Concede permiso para poner datos de interacciones de acciones en tiempo real	Escritura			
PutActions	Concede permiso para incorporar datos de acciones	Escritura	dataset*		
PutEvents	Concede permiso para poner datos de eventos en tiempo real	Write			
PutItems	Otorga permiso para incorporar datos de elementos	Write	dataset*		
PutUsers	Otorga permiso para incorporar datos de usuarios	Escritura	dataset*		
StartRecommender	Otorga permiso para iniciar un recomendador	Escritura	recommender*		
StopRecommender	Otorga permiso para detener un recomendador	Escritura	recommender*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopSolutionVersionCreation	Otorga permiso para detener la creación de versión de una solución	Escritura	solution*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado			
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado			
UpdateCampaign	Concede permiso para actualizar una campaña	Escritura	campaign*		
UpdateDataset	Concede permiso para actualizar un conjunto de datos	Escritura	dataset*		
UpdateMetricAttribution	Otorga permiso para actualizar la atribución de métrica	Escritura	metricAttribution*		
UpdateRecommender	Otorga permiso para actualizar un recomendador.	Escritura	recommender*		
UpdateSolution	Concede permiso para actualizar una solución	Escritura	solution*		

Tipos de recurso definidos por Amazon Personalize

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
schema	`arn:${Partition}:personalize:${Region}:${Account}:schema/${ResourceId}`	
featureTransformation	`arn:${Partition}:personalize:::feature-transformation/${ResourceId}`	
dataset	`arn:${Partition}:personalize:${Region}:${Account}:dataset/${ResourceId}`	
datasetGroup	`arn:${Partition}:personalize:${Region}:${Account}:dataset-group/${ResourceId}`	
datasetImportJob	`arn:${Partition}:personalize:${Region}:${Account}:dataset-import-job/${ResourceId}`	
dataInsightsJob	`arn:${Partition}:personalize:${Region}:${Account}:data-insights-job/${ResourceId}`	
datasetExportJob	`arn:${Partition}:personalize:${Region}:${Account}:dataset-export-job/${ResourceId}`	
dataDeletionJob	`arn:${Partition}:personalize:${Region}:${Account}:data-deletion-job/${ResourceId}`	
solution	`arn:${Partition}:personalize:${Region}:${Account}:solution/${ResourceId}`	

Tipos de recurso	ARN	Claves de condición
campaign	arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}	
eventTracker	arn:${Partition}:personalize:${Region}:${Account}:event-tracker/${ResourceId}	
recipe	arn:${Partition}:personalize:::recipe/${ResourceId}	
algorithm	arn:${Partition}:personalize:::algorithm/${ResourceId}	
batchInferenceJob	arn:${Partition}:personalize:${Region}:${Account}:batch-inference-job/${ResourceId}	
filter	arn:${Partition}:personalize:${Region}:${Account}:filter/${ResourceId}	
recommender	arn:${Partition}:personalize:${Region}:${Account}:recommender/${ResourceId}	
batchSegmentJob	arn:${Partition}:personalize:${Region}:${Account}:batch-segment-job/${ResourceId}	
metricAttribution	arn:${Partition}:personalize:${Region}:${Account}:metric-attribution/${ResourceId}	

Claves de condición de Amazon Personalize

Personalize no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Pinpoint

Amazon Pinpoint (prefijo de servicio: `mobiletargeting`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Pinpoint
- Tipos de recurso definidos por Amazon Pinpoint
- Claves de condición de Amazon Pinpoint

Acciones definidas por Amazon Pinpoint

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApp	Otorga permiso para crear una aplicación.	Escritura	apps*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateCampaign	Otorga permiso para crear una campaña para una aplicación.	Escritura	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Concede permiso para crear una plantilla de email	Escritura	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateExportJob	Otorga permiso para crear un trabajo de exportación que exporta definiciones de punto de conexión a Amazon S3.	Escritura	app*		
CreateImportJob	Otorga permiso para importar definiciones de punto de conexión para crear un segmento.	Escritura	app*		
CreateInAppTemplate	Otorga permiso para crear una plantilla de mensaje dentro de la aplicación	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateJourney	Otorga permiso para crear un recorrido para una aplicación.	Escritura	journeys*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreatePushTemplate	Otorga permiso para crear una plantilla de notificación push.	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecommenderConfiguration	Otorga permiso para crear una configuración de Amazon Pinpoint para un modelo de recomendador.	Escritura	recommenders*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSegment	Otorga permiso para crear un segmento basado en los datos de punto de enlace notificados a Pinpoint por la aplicación. Para permitir que un usuario cree un segmento importando datos de puntos finales desde fuera de Pinpoint, permita la acción mobiletargeting: CreateImportJob	Escritura	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateSmsTemplate	Otorga permiso para crear una plantilla de mensaje sms.	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateVoiceTemplate	Otorga permiso para crear una plantilla de mensaje de voz.	Escritura	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAdmChannel	Otorga permiso para eliminar el canal de ADM de una aplicación.	Escritura	channel*		
DeleteApnsChannel	Otorga permiso para eliminar el canal de una aplicación APNs	Escritura	channel*		
DeleteApnsSandboxChannel	Otorga permiso para eliminar el canal APNs sandbox de una aplicación	Escritura	channel*		
DeleteApnsVoipChannel	Otorga permiso para eliminar el canal APNs VoIP de una aplicación	Escritura	channel*		
DeleteApnsVoipSandboxChannel	Otorga permiso para eliminar el canal sandbox de APNs VoIP de una aplicación	Escritura	channel*		
DeleteApp	Otorga permiso para eliminar una campaña específica.	Escritura	app*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBaiduChannel	Otorga permiso para eliminar el canal de Baidu de una aplicación.	Escritura	channel*		
DeleteCampaign	Otorga permiso para eliminar una campaña específica.	Escritura	campaign*		
DeleteEmailChannel	Otorga permiso para eliminar el canal de correo electrónico de una aplicación.	Escritura	channel*		
DeleteEmailTemplate	Otorga permiso para eliminar una plantilla de correo electrónico o una versión de plantilla de correo electrónico.	Escritura	template*		
DeleteEndpoint	Concede permiso para eliminar un punto de conexión.	Escritura	endpoint*		
DeleteEventStream	Otorga permiso para eliminar la secuencia de eventos de una aplicación.	Escritura	event-stream*		
DeleteGcmChannel	Otorga permiso para eliminar el canal de GCM de una aplicación.	Escritura	channel*		
DeleteInAppTemplate	Otorga permiso para eliminar una plantilla de mensaje dentro de la aplicación o una versión de plantilla de mensaje dentro de la aplicación	Escritura	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteJourney	Otorga permiso para eliminar un recorrido específico.	Escritura	journey*		
DeletePushTemplate	Otorga permiso para eliminar una plantilla de notificación push o una versión de plantilla de notificación push.	Escritura	template*		
DeleteRecommenderConfiguration	Otorga permiso para eliminar una configuración de Amazon Pinpoint para un modelo de recomendador.	Escritura	recommender*		
DeleteSegment	Otorga permiso para eliminar un segmento específico.	Escritura	segment*		
DeleteSmsChannel	Otorga permiso para eliminar el canal de SMS de una aplicación.	Escritura	channel*		
DeleteSmsTemplate	Otorga permiso para eliminar una plantilla de mensaje sms o una versión de plantilla de mensaje sms.	Escritura	template*		
DeleteUserEndpoints	Otorga permiso para eliminar todos los puntos de enlace asociados con un ID de usuario.	Escritura	user*		
DeleteVoiceChannel	Otorga permiso para eliminar el canal de voz de una aplicación.	Escritura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteVoiceTemplate	Otorga permiso para eliminar una plantilla de mensaje de voz o una versión de plantilla de mensaje de voz.	Escritura	template*		
GetAdmChannel	Otorga permiso para recuperar información sobre un canal de Amazon Device Messaging (ADM) de una aplicación.	Lectura	channel*		
GetApnsChannel	Otorga permiso para recuperar información sobre el APNs canal de una aplicación	Lectura	channel*		
GetApnsSandboxChannel	Otorga permiso para recuperar información sobre el canal APNs sandbox de una aplicación	Lectura	channel*		
GetApnsVoipChannel	Otorga permiso para recuperar información sobre el canal APNs VoIP de una aplicación	Lectura	channel*		
GetApnsVoipSandboxChannel	Otorga permiso para recuperar información sobre el canal sandbox de APNs VoIP de una aplicación	Lectura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetApp	Otorga permiso para recuperar información acerca de una aplicación específica en su cuenta de Amazon Pinpoint.	Lectura	app*		
GetApplicationDateRangeKpi	Otorga permiso para recuperar (consulta) datos previamente agregados para una métrica estándar que se aplica a una aplicación.	Lectura	application-metrics*		
GetApplicationSettings	Otorga permiso para recuperar la configuración pequeña (predeterminada) de una aplicación.	Enumeración	app*		
GetApps	Otorga permiso para recuperar una lista de aplicaciones en su cuenta de Amazon Pinpoint.	Lectura	apps*		
GetBaiduChannel	Otorga permiso para recuperar información sobre el canal de Baidu de una aplicación.	Lectura	channel*		
GetCampaign	Otorga permiso para recuperar información acerca de un trabajo de firma específico.	Lectura	campaign*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCampaignActivities	Otorga permiso para recuperar información acerca de las actividades realizadas por una campaña.	Enumeración	campaign*		
GetCampaignDateRangeKpi	Otorga permiso para recuperar (consulta) datos previamente agregados para una métrica estándar que se aplica a una campaña.	Lectura	campaign-metrics*		
GetCampaignVersion	Otorga permiso para recuperar información sobre una versión de campaña específica.	Lectura	campaign*		
GetCampaignVersions	Otorga permiso para recuperar información acerca de las versiones actual y anteriores de una campaña.	Enumeración	campaign*		
GetCampaigns	Otorga permiso para recuperar información acerca de todas las campañas de una aplicación.	Enumeración	app*		
GetChannels	Otorga permiso para obtener información de todos los canales de su aplicación.	Enumeración	channels*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEmailChannel	Otorga permiso para obtener información sobre el canal de correo electrónico de una aplicación.	Lectura	channel*		
GetEmailTemplate	Otorga permiso para recuperar información sobre una versión específica o activa de una plantilla de correo electrónico.	Lectura	template*		
GetEndpoint	Otorga permiso para recuperar información acerca de un trabajo de firma específico.	Lectura	endpoint*		
GetEventStream	Otorga permiso para recuperar información acerca de la secuencia de eventos de una aplicación.	Lectura	event-stream*		
GetExportJob	Otorga permiso para obtener información sobre un trabajo de exportación específico.	Lectura	export-job*		
GetExportJobs	Otorga permiso para recuperar una lista de todos los trabajos de exportación de una aplicación.	Enumeración	app*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGcmChannel	Otorga permiso para recuperar información acerca del canal de GCM de una aplicación.	Lectura	channel*		
GetImportJob	Otorga permiso para recuperar información acerca de un trabajo de firma específico.	Lectura	import-job*		
GetImportJobs	Otorga permiso para recuperar información acerca de todos los trabajos de importación referentes a una aplicación.	Enumeración	app*		
GetInAppMessages	Otorga permiso para recuperar mensajes dentro de la aplicación para el ID de punto de conexión determinado.	Lectura	app*		
GetInAppTemplate	Otorga permiso para recuperar información sobre una versión específica o activa de una plantilla de mensaje dentro de la aplicación	Lectura	template*		
GetJourney	Otorga permiso para recuperar información acerca de un trabajo de firma específico.	Lectura	journey*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetJourneyDateRangeKpi	Otorga permiso para recuperar (consulta) datos previamente agregados para una métrica de interacción estándar que se aplica a un viaje.	Lectura	journey-metrics*		
GetJourneyExecutionActivityMetrics	Otorga permiso para recuperar (consultas) datos previamente agregados para una métrica de ejecución estándar que se aplica a una actividad de viaje.	Lectura	journey-execution-activity-metrics*		
GetJourneyExecutionMetrics	Otorga permiso para recuperar (consultas) datos previamente agregados para una métrica de ejecución estándar que se aplica a un viaje.	Lectura	journey-execution-metrics*		
GetJourneyRunExecutionActivityMetrics	Otorga permiso para recuperar (consultas) datos previamente agregados para una métrica de ejecución estándar que se aplica a una actividad de viaje para una única ejecución de viaje.	Lectura	journey*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetJourneyRunExecutionMetrics	Otorga permiso para recuperar (consultas) datos previamente agregados para una métrica de ejecución estándar que se aplica a un viaje para una única ejecución de viaje.	Lectura	journey*		
GetJourneyRuns	Otorga permiso para recuperar información sobre todas las ejecuciones de viajes para un viaje.	Enumeración	journey*		
GetPushTemplate	Otorga permiso para recuperar información sobre una versión específica o activa de una plantilla de notificación push.	Lectura	template*		
GetRecommenderConfiguration	Otorga permiso para recuperar información sobre una configuración de Amazon Pinpoint para un modelo de recomendación.	Lectura	recommender*		
GetRecommenderConfigurations	Otorga permiso para recuperar información sobre todas las configuraciones de modelos de recomendación asociadas a una cuenta de Amazon Pinpoint.	Enumeración	recommenders*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetReports [solo permiso]	Otorga permiso a la segmentación móvil: GetReports	Lectura	reports*		
GetSegment	Otorga permiso para recuperar información acerca de un trabajo de firma específico.	Lectura	segment*		
GetSegmentExportJobs	Otorga permiso para recuperar información acerca de trabajos que exportan definiciones de punto de conexión de segmentos a Amazon S3.	Enumeración	segment*		
GetSegmentImportJobs	Otorga permiso para recuperar información sobre los trabajos que crean segmentos mediante la importación de definiciones de punto de conexión desde	List	segment*		
GetSegmentVersion	Otorga permiso para recuperar información sobre una versión de segmento específica.	Lectura	segment*		
GetSegmentVersions	Otorga permiso para recuperar información acerca de las versiones actual y anteriores de un segmento.	Enumeración	segment*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSegments	Otorga permiso para recuperar información sobre los segmentos de una aplicación.	Enumeración	app*		
GetSmsChannel	Otorga permiso para obtener información sobre el canal de SMS de una aplicación.	Lectura	channel*		
GetSmsTemplate	Otorga permiso para recuperar información sobre una versión específica o activa de una plantilla de mensaje sms.	Lectura	template*		
GetUserEndpoints	Otorga permiso para recuperar información sobre los puntos de enlace que están asociados con un ID de usuario.	Lectura	user*		
GetVoiceChannel	Otorga permiso para obtener información sobre el canal de voz de una aplicación.	Lectura	channel*		
GetVoiceTemplate	Otorga permiso para recuperar información sobre una versión específica o activa de una plantilla de mensaje de voz.	Lectura	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListJourneys	Otorga permiso para recuperar información sobre todos los viajes de una aplicación.	Enumeración	app*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	app		
			campaign		
			journey		
			segment		
			template		
ListTemplateVersions	Otorga permiso para recuperar todas las versiones de una plantilla específica.	Enumeración	template*		
ListTemplates	Otorga permiso para recuperar metadatos sobre las plantillas consultadas.	Enumeración	templates*		
PhoneNumberValidate	Otorga permiso para obtener metadatos de un número de teléfono, como el tipo de número (móvil, fijo o VoIP), ubicación y proveedor.	Lectura	phone-number-validate*		
PutEventStream	Otorga permiso para crear o actualizar un evento de una aplicación.	Escritura	event-stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutEvents	Otorga permiso para crear o actualizar eventos de una aplicación.	Escritura	events*		
RemoveAttributes	Otorga permiso para eliminar los atributos de una aplicación.	Escritura	attribute*		
SendMessages	Otorga permiso para enviar un mensaje SMS o una notificación push a puntos de enlace específicos.	Escritura	messages*		
SendOTPMessage	Otorga permiso para enviar un código OTP a un usuario de su aplicación	Escritura	otp*		
SendUsersMessages	Otorga permiso para enviar un mensaje SMS o una notificación de inserción a todos los puntos de enlace asociados a un ID de usuario concreto.	Escritura	messages*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	app		
			campaign		
			journey		
			segment		
			template		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateAdmChannel	Otorga permiso para actualizar el canal de Amazon Device Messaging (ADM) de una aplicación.	Escritura	channel*		
UpdateApnsChannel	Otorga permiso para actualizar el canal del servicio de notificaciones push de Apple (APNs) de una aplicación	Escritura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApnsSandboxChannel	Otorga permiso para actualizar el canal limitado del servicio de notificaciones push de Apple (APNs) para una aplicación	Escritura	channel*		
UpdateApnsVoipChannel	Otorga permiso para actualizar el canal VoIP del servicio de notificaciones push de Apple (APNs) para una aplicación	Escritura	channel*		
UpdateApnsVoipSandboxChannel	Otorga permiso para actualizar el canal aislado VoIP del servicio de notificaciones push de Apple (APNs) para una aplicación	Escritura	channel*		
UpdateApplicationSettings	Otorga permiso para actualizar la configuración pequeña (predeterminada) de una aplicación.	Escritura	app*		
UpdateBaiduChannel	Otorga permiso para actualizar el canal de Baidu para una aplicación.	Escritura	channel*		
UpdateCampaign	Otorga permiso para actualizar una campaña específica.	Escritura	campaign*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailChannel	Otorga permiso para actualizar los detalles de un AppInstanceUser (Usuario de instancia de aplicaciones).	Escritura	channel*		
UpdateEmailTemplate	Otorga permiso para actualizar una plantilla de correo electrónico específica con la misma versión o genera una nueva versión.	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEndpoint	Otorga permiso para crear un punto de conexión o actualizar la información sobre uno.	Escritura	endpoint*		
UpdateEndpointsBatch	Otorga permiso para crear o actualizar puntos de conexión como una operación por lotes.	Escritura	app*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGcmChannel	Otorga permiso para actualizar la clave de API de Firebase Cloud Messaging (FCM) o Google Cloud Messaging (GCM), que permiten enviar notificaciones de inserción a la aplicación de Android.	Escritura	channel*		
UpdateInAppTemplate	Otorga permiso para actualizar una plantilla de mensaje dentro de la aplicación específica con la misma versión o generar una nueva versión	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourney	Otorga permiso para actualizar un viaje específico.	Escritura	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourneyState	Otorga permiso para actualizar un estado de recorrido específico.	Escritura	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePushTemplate	Otorga permiso para actualizar una plantilla de notificación push específica con la misma versión o genera una nueva versión.	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateRecommenderConfiguration	Otorga permiso para actualizar una configuración de Amazon Pinpoint para un modelo de recomendador.	Escritura	recommender*		
UpdateSegment	Otorga permiso para actualizar un segmento específico.	Escritura	segment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSmsChannel	Otorga permiso para actualizar el canal de SMS de una aplicación.	Escritura	channel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSmsTemplate	Otorga permiso para actualizar una plantilla de mensaje sms específica con la misma versión o genera una nueva versión.	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTemplateActiveVersion	Otorga permiso para actualizar el parámetro de versión activa de una plantilla específica.	Escritura	template*		
UpdateVoiceChannel	Otorga permiso para actualizar el canal de voz de una aplicación.	Escritura	channel*		
UpdateVoiceTemplate	Otorga permiso para actualizar una plantilla de mensaje de voz específica con la misma versión o genera una nueva versión.	Escritura	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyOTPMessage	Otorga permiso para comprobar la validez de las contraseñas de un solo uso () OTPs	Escritura	verify-otp*		

Tipos de recurso definidos por Amazon Pinpoint

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
app	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
apps	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/*`	
campaign	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}`	aws:ResourceTag/${TagKey}
journey	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}`	aws:ResourceTag/${TagKey}
journeys	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys`	
segment	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/segments/${SegmentId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:mobiletargeting:${Region}:${Account}:templates/${TemplateName}/${TemplateType}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
templates	arn:${Partition}:mobiletargeting:${Region}:${Account}:templates	
recommender	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/${RecommenderId}	
recommenders	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/*	
phone-number-validate	arn:${Partition}:mobiletargeting:${Region}:${Account}:phone/number/validate	
channels	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels	
channel	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels/${ChannelType}	
event-stream	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/eventstream	
events	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/events	
messages	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/messages	

Tipos de recurso	ARN	Claves de condición
verify-otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/verify-otp	
otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/otp	
attribute	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/attributes/${AttributeType}	
user	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/users/${UserId}	
endpoint	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/endpoints/${EndpointId}	
import-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/import/${JobId}	
export-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/export/${JobId}	
application-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/kpis/daterange/${KpiName}	
campaign-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}/kpis/daterange/${KpiName}	

Tipos de recurso	ARN	Claves de condición
journey-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/kpis/daterange/${KpiName}	
journey-execution-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/execution-metrics	
journey-execution-activity-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/activities/${JourneyActivityId}/execution-metrics	
reports	arn:${Partition}:mobiletargeting:${Region}:${Account}:reports	

Claves de condición de Amazon Pinpoint

Amazon Pinpoint define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave que está presente en la solicitud que el usuario realiza al servicio Pinpoint.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena
aws:TagKeys	Filtra el acceso mediante la lista de todos los nombres de clave de etiqueta presentes en la solicitud que el usuario realiza al servicio Pinpoint.	ArrayOfString

Acciones, recursos y claves de condición para Amazon Pinpoint Email Service

Amazon Pinpoint Email Service (prefijo de servicio: `ses`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Pinpoint Email Service
- Tipos de recurso definidos por Amazon Pinpoint Email Service
- Claves de condición de Amazon Pinpoint Email Service

Acciones definidas por Amazon Pinpoint Email Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfigurationSet	Otorga permiso para crear un conjunto de configuración	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Concede permiso para crear un destino para eventos de conjunto de configuración	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateDedicatedIpPool	Concede permiso para crear un grupo de direcciones IP dedicadas nuevo	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Concede permiso para crear una prueba de colocación predictiva en la bandeja de entrada nueva	Write	identity*		
				ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Concede permiso para iniciar el proceso de verificación de una identidad de correo electrónico	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Concede permiso para eliminar un conjunto de configuración existente	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Concede permiso para eliminar un destino de evento	Write	configuration-set*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Concede permiso para eliminar un grupo de IP dedicadas	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Otorga permiso para eliminar una identidad de correo electrónico verificada previamente	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Otorga permiso para obtener información sobre el estado y las capacidades del envío de correo electrónico	Read		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBlacklistReports	Otorga permiso para recuperar una lista de las listas de denegación en las que aparecen sus direcciones IP dedicadas.	Read		ses:ApiVersion	
GetConfigurationSet	Concede permiso para obtener información sobre un conjunto de configuración existente	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Concede permiso para recuperar una lista de destinos de eventos que están asociados con un conjunto de configuración	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Concede permiso para obtener información sobre una dirección IP dedicada	Read		ses:ApiVersion	
GetDedicatedIps	Otorga permiso para enumerar las direcciones IP dedicadas asociadas a su cuenta	Read	dedicated-ip-pool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Concede permiso para obtener el estado del panel de capacidad de entrega	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Concede permiso para recuperar los resultados de una prueba de colocación predictiva en la bandeja de entrada	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Concede permiso para recuperar todos los datos de capacidad de entrega de una campaña específica	Read		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDomainStatisticsReport	Concede permiso para recuperar la ubicación de la bandeja de entrada y las tasas de interacción de los dominios que utiliza para enviar correos electrónicos	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Otorga permiso para obtener información sobre una identidad específica asociada a su cuenta	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Otorga permiso para enumerar todos los conjuntos de configuración asociados a su cuenta	List		ses:ApiVersion	
ListDedicatedIpPools	Otorga permiso para enumerar todos los grupos de IP dedicadas que existen en su cuenta	List		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeliverabilityTestReports	Otorga permiso para recuperar una lista de las pruebas predictivas de ubicación de la bandeja de entrada que haya realizado, independientemente de sus estados	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Otorga permiso para recuperar datos de capacidad de entrega de todas las campañas que utilizaron un dominio específico a fin de enviar correos electrónicos durante un intervalo de tiempo especificado	Read		ses:ApiVersion	
ListEmailIdentities	Otorga permiso para enumerar todas las identidades de correo electrónico asociadas a su cuenta	List		ses:ApiVersion	
ListTagsForResource	Otorga permiso para recuperar una lista de las etiquetas (claves y valores) asociadas a un recurso específico	Read	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion	
PutAccountDedicatedIpWarmupAttributes	Concede permiso para habilitar o desactivar la característica de preparación automática para direcciones IP dedicadas	Write		ses:ApiVersion	
PutAccountSendingAttributes	Otorga permiso para habilitar o desactivar la capacidad de su cuenta para enviar correos electrónicos	Write		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Concede permiso para asociar un conjunto de configuración a un grupo de IP dedicadas	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Concede permiso para habilitar o desactivar la recopilación de métricas de reputación para los correos electrónicos que envía a través de un conjunto de configuración determinado	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConfigurationSetSendingOptions	Concede permiso para habilitar o desactivar el envío de correos electrónicos para mensajes que utilizan un conjunto de configuración determinado	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Otorga permiso para especificar un dominio personalizado que se utilizará para los elementos de seguimiento de apertura y clic en el correo electrónico que envíe mediante un conjunto de configuración determinado	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Concede permiso para mover una dirección IP dedicada a un grupo de IP dedicadas existente	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Otorga permiso para habilitar atributos de preparación de IP dedicadas	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutDeliverabilityDashboardOption	Concede permiso para habilitar o desactivar el panel de capacidad de entrega	Write		ses:ApiVersion	
PutEmailIdentityDkimAttributes	Concede permiso para habilitar o desactivar la autenticación DKIM para una identidad de correo electrónico	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Otorga permiso para habilitar o desactivar el reenvío de comentarios para una identidad	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Concede permiso para habilitar o desactivar la configuración de dominio MAIL FROM personalizada para una identidad de correo electrónico	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
SendEmail	Concede permiso para enviar un mensaje de correo electrónico	Write	identity*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	Concede permiso para agregar una o varias etiquetas (claves y valores) a un recurso especificado	Etiquetado	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una o más etiquetas (claves y valores) de un recurso especificado	Etiquetado	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Concede permiso para actualizar la configuración de un destino de eventos para un conjunto de configuración	Write	configuration-set*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Tipos de recurso definidos por Amazon Pinpoint Email Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Pinpoint Email Service

Amazon Pinpoint Email Service define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString
ses:ApiVersion	Filtra acciones basadas en la versión de la API de SES	Cadena
ses:FeedbackAddress	Filtra acciones en función de la dirección "Return-Path" (Ruta de devolución), que especifica dónde se envían los mensajes rebotados y las reclamaciones mediante el reenvío de retroalimentación por correo electrónico	Cadena

Claves de condición	Descripción	Tipo
ses:FromAddress	Filtra acciones en función de la dirección "From" (Origen) de un mensaje	Cadena
ses:FromDisplayName	Filtra acciones en función de la dirección "From" (Origen) que se utiliza como nombre de visualización de un mensaje	Cadena
ses:Recipients	Filtra acciones en función de las direcciones de los destinatarios de un mensaje, que incluyen las direcciones "To" (Destino), "CC" (Copia) y "BCC" (Copia oculta).	ArrayOfString

Acciones, recursos y claves de condición para Amazon Pinpoint SMS and Voice Service

Amazon Pinpoint SMS and Voice Service (prefijo de servicio: `sms-voice`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Pinpoint SMS and Voice Service
- Tipos de recurso definidos por Amazon Pinpoint SMS and Voice Service
- Claves de condición de Amazon Pinpoint SMS and Voice Service

Acciones definidas por Amazon Pinpoint SMS and Voice Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfigurationSet	Crea un nuevo conjunto de configuración. Después de crear el conjunto de configuración, puede agregar uno o varios destinos de eventos.	Write			
CreateConfigurationSetEventDestination	Crea un nuevo destino de eventos en un conjunto de configuración.	Write			iam:PassRole
DeleteConfigurationSet	Elimina un conjunto de configuración existente.	Write			
DeleteConfigurationSetEventDestination	Elimina un destino de eventos en un conjunto de configuración.	Write			
GetConfigurationSetEventDestinations	Obtiene información acerca de un destino de eventos, incluidos los tipos de eventos que comunica, el nombre de recurso de Amazon (ARN) del destino y el nombre del destino de eventos.	Read			
ListConfigurationSets	Devuelve una lista de conjuntos de configuración. Esta operación solo devuelve	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	los conjuntos de configuración asociados con su cuenta en la Región de AWS actual.				
SendVoiceMessage	Cree un nuevo mensaje de voz y lo envía al número de teléfono de un destinatario.	Write			
UpdateConfigurationSetEventDestination	Actualiza un destino de eventos en un conjunto de configuración. Un destino de eventos es una ubicación en la que publica información acerca de sus llamadas de voz. Por ejemplo, puedes registrar un evento en un CloudWatch destino de Amazon cuando se produce un error en una llamada.	Escritura			iam:PassRole

Tipos de recurso definidos por Amazon Pinpoint SMS and Voice Service

El servicio de SMS y voz de Amazon Pinpoint no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso al servicio de SMS y voz de Amazon Pinpoint, especifique `"Resource": "*"` en su política.

Claves de condición de Amazon Pinpoint SMS and Voice Service

Pinpoint SMS Voice no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Polly

Amazon Polly (prefijo de servicio: `polly`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Polly
- Tipos de recurso definidos por Amazon Polly
- Claves de condición de Amazon Polly

Acciones definidas por Amazon Polly

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLexicon	Otorga permiso para eliminar el léxico de pronunciación especificado almacenado en un Región de AWS	Escritura	lexicon*		
DescribeVoices	Concede permiso para describir la lista de voces que están disponibles para su uso cuando se solicita la síntesis de voz	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLexicon	Otorga permiso para recuperar el contenido del léxico de pronunciación especificado almacenado en un Región de AWS	Lectura	lexicon*		
GetSpeechSynthesisTask	Concede permiso para obtener información acerca de una tarea de síntesis de voz específica	Lectura			
ListLexicons	Otorga permiso para enumerar los léxicos de pronunciación almacenados en un Región de AWS	Enumeración			
ListSpeechSynthesisTasks	Concede permiso para enumerar las tareas de síntesis de voz solicitadas	Enumeración			
PutLexicon	Otorga permiso para almacenar un léxico de pronunciación en un Región de AWS	Escritura	lexicon*		
StartSpeechSynthesisTask	Concede permiso para sintetizar entradas largas en la ubicación de S3 proporcionada	Escritura	lexicon		s3:PutObject
SynthesizeSpeech	Concede permiso para sintetizar voz	Lectura	lexicon		

Tipos de recurso definidos por Amazon Polly

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Claves de condición de Amazon Polly

Polly no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Price List

AWS La lista de precios (prefijo de servicio:`pricing`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Price List
- Tipos de recursos definidos por AWS Price List

- Claves de condición para AWS Price List

Acciones definidas por AWS Price List

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeServices	Concede permiso para recuperar detalles del servicio para todos los servicios (paginados) (si no se ha establecido serviceCode) o los detalles de servicio para un servicio determinado (si se establece serviceCode)	Lectura			
GetAttributeValues	Concede permiso para recuperar todos los valores (paginados) posibles de un determinado atributo	Lectura			
GetPriceListFileUrl	Concede permiso para recuperar la URL de un archivo de lista de precios para los parámetros en cuestión	Lectura			
GetProducts	Concede permiso para recuperar todos los productos coincidentes con los criterios de búsqueda determinada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPriceLists	Concede permiso para enumerar todas las listas de precios elegibles (paginadas) para los parámetros en cuestión	Lectura			

Tipos de recursos definidos por AWS Price List

AWS La lista de precios no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Price List, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Price List

Price List no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de AWS Private CA Connector for Active Directory

AWS El CA Connector privado para Active Directory (prefijo de servicio:`pca-connector-ad`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Private CA Connector for Active Directory
- Tipos de recursos definidos por AWS Private CA Connector for Active Directory
- Claves de condición de AWS Private CA Connector for Active Directory

Acciones definidas por AWS Private CA Connector for Active Directory

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnector	Concede permiso para crear un conector en su cuenta	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:I

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ssueCertificate ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
CreateDirectoryRegistration	Otorga permiso para crear una DirectoryRegistration en su cuenta	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:DescribeDirectories
CreateServicePrincipalName	Otorga permiso para crear un ServicePrincipalName para un DirectoryRegistration	Escritura	Directory Registration*		ds:UpdateAuthorizedApplication
CreateTemplate	Concede permiso para crear una plantilla para un conector	Escritura	Connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTemplateGroupAccessControlEntry	Otorga permiso para crear un TemplateGroupAccessControlEntry para una plantilla	Escritura	Template*		
DeleteConnector	Concede permiso para eliminar un conector de su cuenta	Escritura	Connector*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteDirectoryRegistration	Otorga permiso para eliminar una DirectoryRegistration de tu cuenta	Escritura	DirectoryRegistration*		ds:UnauthorizeApplication ds:UpdateAuthorizedApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteServicePrincipalName	Otorga permiso para eliminar un ServicePrincipalName para un DirectoryRegistration	Escritura	DirectoryRegistration*		ds:UpdateAuthorizedApplication
DeleteTemplate	Concede permiso para eliminar una plantilla de un conector	Escritura	Template*		
DeleteTemplateGroupAccessControlEntry	Otorga permiso para eliminar un TemplateGroupAccessControlEntry para una plantilla	Escritura	Template*		
GetConnector	Concede permiso para obtener un conector en su cuenta	Lectura	Connector*		
GetDirectoryRegistration	Otorga permiso para acceder a una DirectoryRegistration en tu cuenta	Lectura	DirectoryRegistration*		
GetServicePrincipalName	Otorga permiso ServicePrincipalName para obtener un DirectoryRegistration	Lectura	DirectoryRegistration*		
GetTemplate	Concede permiso para obtener una plantilla para un conector	Lectura	Template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTemplateGroupAccessControlEntry	Otorga permiso para obtener un TemplateGroupAccessControlEntry para una plantilla	Lectura	Template*		
ListConnectors	Concede permiso para enumerar los conectores en su cuenta	Enumeración			
ListDirectoryRegistrations	Otorga permiso para Directory Registrations incluirla en tu cuenta	Enumeración			
ListServicePrincipalNames	Otorga permiso para incluirlo en ServicePrincipalNames una lista DirectoryRegistration	Enumeración	DirectoryRegistration*		
ListTagsForResource	Otorga permiso para incluir las etiquetas de un pca-connector-ad recurso de su cuenta	Lectura			
ListTemplateGroupAccessControlEntries	Otorga permiso para incluirlas TemplateGroupAccessControlEntries en una plantilla	Enumeración	Template*		
ListTemplates	Concede permiso para enumerar las plantillas para un conector	Enumeración	Connector*		
TagResource	Otorga permiso para etiquetar un pca-connector-ad recurso en su cuenta	Etiquetado	Connector		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Directory Registration		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar la etiqueta de un pca-connector-ad recurso de tu cuenta	Etiquetado	Connector		
			Directory Registration		
			Template		
				aws:TagKeys	
UpdateTemplate	Concede permiso para actualizar una plantilla para un conector	Escritura	Template*		
UpdateTemplateGroupAccessControlEntry	Otorga permiso TemplateGroupAccessControlEntry para actualizar una plantilla	Escritura	Template*		

Tipos de recursos definidos por AWS Private CA Connector for Active Directory

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Connector	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}
Directory Registration	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:directory-registration/${DirectoryId}`	aws:ResourceTag/${TagKey}
Template	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Private CA Connector for Active Directory

AWS El conector de CA privado para Active Directory define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso según las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para el Conector de AWS Private CA para SCEP

AWS El CA Connector privado para SCEP (prefijo de servicio:`pca-connector-scep`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el Conector de AWS Private CA para SCEP
- Tipos de recursos definidos por el Conector de AWS Private CA para SCEP
- Claves de condición del Conector de AWS Private CA para SCEP

Acciones definidas por el Conector de AWS Private CA para SCEP

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateChallenge	Concede permiso para crear un desafío para un conector	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Concede permiso para crear un conector SCEP en la cuenta	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteChallenge	Concede permiso para eliminar un desafío para un conector	Escritura	Challenge*		
DeleteConnector	Concede permiso para eliminar un conector SCEP en la cuenta	Escritura	Connector*		
GetChallengeMetadata	Concede permiso para obtener un desafío para un conector	Lectura	Challenge*		
GetChallengePassword	Concede permiso para obtener la contraseña de un desafío para un conector	Lectura	Challenge*		
GetConnector	Concede permiso para obtener un conector SCEP en la cuenta	Lectura	Connector*		
ListChallengeMetadata	Concede permiso para enumerar desafíos para un conector	Enumeración			
ListConnectors	Concede permiso para enumerar los conectores SCEP en la cuenta	Enumeración			
ListTagsForResource	Otorga permiso para incluir las etiquetas de un pca-connector-scep recurso en tu cuenta	Lectura			
TagResource		Etiquetado	Challenge		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para etiquetar un pca-connector-scep recurso en tu cuenta		Connector		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar la etiqueta de un pca-connector-scep recurso de tu cuenta	Etiquetado	Challenge		
			Connector		
				aws:TagKeys	

Tipos de recursos definidos por el Conector de AWS Private CA para SCEP

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Challenge	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}/challenge/${ChallengeId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
Connector	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}

Claves de condición del Conector de AWS Private CA para SCEP

AWS Private CA Connector for SCEP define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Private Certificate Authority

AWS La autoridad de certificación privada (prefijo de servicio:`acm-pca`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Private Certificate Authority
- Tipos de recursos definidos por AWS Private Certificate Authority
- Claves de condición para AWS Private Certificate Authority

Acciones definidas por AWS Private Certificate Authority

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCertificateAuthority	Otorga permiso para crear una CA AWS privada y su clave privada y configuración asociadas	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	Otorga permiso para crear un informe de auditoría para una CA AWS privada	Escritura	certificate-authority*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePermission	Otorga permiso para crear un permiso para una CA AWS privada	Administración de permisos	certificate-authority*		
DeleteCertificateAuthority	Otorga permiso para eliminar una CA AWS privada y su clave privada y configuración asociadas	Escritura	certificate-authority*		
DeletePermission	Otorga permiso para eliminar un permiso para una CA AWS privada	Administración de permisos	certificate-authority*		
DeletePolicy	Otorga permiso para eliminar la política de una CA AWS privada	Administración de permisos	certificate-authority*		
DescribeCertificateAuthority	Otorga permiso para devolver una lista de los campos de configuración y estado contenidos en la CA AWS privada especificada	Lectura	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Otorga permiso para devolver el estado y la información sobre un informe de auditoría de una CA AWS privada	Lectura	certificate-authority*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCertificate	Otorga permiso para recuperar un certificado de CA AWS privada y una cadena de certificados para la autoridad de certificación especificada por un ARN	Lectura	certificate-authority*		
GetCertificateAuthorityCertificate	Otorga permiso para recuperar un certificado de CA AWS privada y una cadena de certificados para la autoridad de certificación especificada por un ARN	Lectura	certificate-authority*		
GetCertificateAuthorityCsr	Concede permiso para recuperar una solicitud de firma de certificado (CSR) de una CA AWS privada para la autoridad de certificación especificada por un ARN	Lectura	certificate-authority*		
GetPolicy	Otorga permiso para recuperar la política en una CA privada AWS	Lectura	certificate-authority*		
ImportCertificateAuthorityCertificate	Otorga permiso para importar un SSL/TLS certificado a una CA AWS privada para usarlo como certificado de CA de una CA AWS privada	Escritura	certificate-authority*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
IssueCertificate	Otorga permiso para emitir un certificado de CA AWS privada	Escritura	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	Otorga permiso para recuperar una lista de la entidad emisora ARNs de certificados AWS privada y un resumen del estado de cada entidad emisora de certificados de la cuenta llamante	Enumeración			
ListPermissions	Otorga permiso para enumerar los permisos que se han aplicado a la autoridad de certificación de CA AWS privada	Lectura	certificate-authority*		
ListTags	Otorga permiso para enumerar las etiquetas que se han aplicado a la entidad emisora de certificados de CA AWS privada	Lectura	certificate-authority*		
PutPolicy	Otorga permiso para poner una política en una CA AWS privada	Administración de permisos	certificate-authority*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreCertificateAuthority	Otorga permiso para restaurar una CA AWS privada desde el estado eliminado al estado en el que se encontraba cuando se eliminó	Escritura	certificate-authority*		
RevokeCertificate	Otorga permiso para revocar un certificado emitido por una CA AWS privada	Escritura	certificate-authority*		
TagCertificateAuthority	Otorga permiso para añadir una o más etiquetas a una CA AWS privada	Etiquetado	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCertificateAuthority	Otorga permiso para eliminar una o más etiquetas de una CA AWS privada	Etiquetado	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	Otorga permiso para actualizar la configuración de una CA AWS privada	Escritura	certificate-authority*		

Tipos de recursos definidos por AWS Private Certificate Authority

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Private Certificate Authority

AWS La autoridad de certificación privada define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
acm-pca:TemplateArn	Filtra el acceso en función del ARN de la plantilla de certificado utilizada en la solicitud de emisión de certificado	ARN
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS PrivateLink

AWS PrivateLink (prefijo de servicio:`vpce`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS PrivateLink
- Tipos de recursos definidos por AWS PrivateLink
- Claves de condición de AWS PrivateLink

Acciones definidas por AWS PrivateLink

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowMultiRegion [solo permiso]	Otorga permiso para administrar configuraciones de servicios de puntos finales de VPC y puntos de enlace de VPC de varias regiones	Escritura			

Tipos de recursos definidos por AWS PrivateLink

AWS PrivateLink no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS PrivateLink, especifique `"Resource": "*"` en su política.

Claves de condición de AWS PrivateLink

Los puntos finales de VPC no tienen claves de contexto específicas de un servicio que puedan usarse en el elemento de las `Condition` declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Proton

AWS Proton (prefijo de servicio:`proton`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Proton
- Tipos de recursos definidos por AWS Proton
- Claves de condición para AWS Proton

Acciones definidas por AWS Proton

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptEnvironmentAccountConnection	Otorga permiso para rechazar una solicitud de conexión de cuenta de entorno desde otra cuenta de entorno	Escritura	environment-account-connection*		
CancelComponentDeployment	Otorga permiso para cancelar una implementación de componentes.	Escritura	component*		
CancelEnvironmentDeployment	Otorga permiso para cancelar una implementación de entorno	Write	environment*		
				proton:EnvironmentTemplate	
CancelServiceInstanceDeployment	Otorga permiso para cancelar una implementación de instancia de servicio	Write	service-instance*		
				proton:ServiceTemplate	
CancelServicePipel		Escritura	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ineDeployment	Otorga permiso para cancelar una implementación de canalización de servicio			proton:ServiceTemplate	
CreateComponent	Otorga permiso para crear componentes.	Escritura	component*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironment	Concede permiso para crear un entorno.	Write	environment*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} proton:EnvironmentTemplate	
CreateEnvironmentAccountConnection	Otorga permiso para crear una conexión de cuenta de entorno	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironmentTemplate	Otorga permiso para crear una plantilla de entorno.	Escritura	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMajorVersion	Otorga permiso para crear una versión principal de la plantilla de entorno. OBSOLETO: utilícelo en su lugar CreateEnvironmentTemplateVersion	Escritura	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMinorVersion	Otorga permiso para crear una versión secundaria de la plantilla de entorno. OBSOLETO: utilícelo en su lugar CreateEnvironmentTemplateVersion	Escritura	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironmentTemplateVersion	Otorga permiso para crear una versión de la plantilla de entorno	Escritura	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRepository	Otorga permiso para crear un repositorio	Escritura	repository*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Otorga permiso para crear un servicio.	Escritura	service*		codestar-connections:PassConnection

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceInstance	Concede permiso para crear una instancia de servicio	Escritura	service-instance*		
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceSyncConfig	Concede permiso para crear una configuración de sincronización de servicio	Escritura			
CreateServiceTemplate	Otorga permiso para crear una plantilla de servicio.	Escritura	service-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMajorVersion	Otorga permiso para crear una versión principal de la plantilla de servicio OBSOLETO: utilícelo en su lugar CreateServiceTemplateVersion	Escritura	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMinorVersion	Otorga permiso para crear una versión secundaria de la plantilla de servicio. OBSOLETO: utilícelo en su lugar CreateServiceTemplateVersion	Escritura	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateVersion	Otorga permiso para crear una versión de la plantilla de servicio	Escritura	service-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTemplateSyncConfig	Otorga permiso para crear una configuración de plantilla sincronizada	Escritura			
DeleteAccountRoles	Otorga permiso para eliminar roles de cuenta. OBSOLETO: utilícelo en su lugar UpdateAccountSettings	Escritura			
DeleteComponent	Otorga el permiso para eliminar componentes	Escritura	component*		
DeleteDeployment	Concede permiso para eliminar una implementación	Escritura	deployment*		
DeleteEnvironment	Concede permiso para eliminar un entorno.	Write	environment*		
				proton:EnvironmentTemplate	
DeleteEnvironmentAccountConnection	Otorga permiso para eliminar una conexión de cuenta de entorno	Write	environment-account-connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEnvironmentTemplate	Otorga permiso para eliminar una plantilla de entorno.	Escritura	environment-template*		
DeleteEnvironmentTemplateMajorVersion	Otorga permiso para eliminar una versión principal de la plantilla de entorno. OBSOLETO: utilícelo en su lugar DeleteEnvironmentTemplateVersion	Escritura	environment-template*		
DeleteEnvironmentTemplateMinorVersion	Otorga permiso para eliminar una versión secundaria de la plantilla de entorno. OBSOLETO: utilícelo en su lugar DeleteEnvironmentTemplateVersion	Escritura	environment-template*		
DeleteEnvironmentTemplateVersion	Otorga permiso para eliminar una versión de la plantilla de entorno	Escritura	environment-template*		
DeleteRepository	Otorga permiso para eliminar un repositorio	Escritura	repository*		
DeleteService	Otorga permiso para eliminar un servicio.	Escritura	service*		
				proton:ServiceTemplate	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteServiceSyncConfig	Concede permiso para eliminar una configuración de sincronización de servicio	Escritura			
DeleteServiceTemplate	Otorga permiso para eliminar una plantilla de servicio.	Escritura	service-template*		
DeleteServiceTemplateMajorVersion	Otorga permiso para eliminar una versión principal de la plantilla de servicio. OBSOLETO: utilícelo en su lugar DeleteServiceTemplateVersion	Escritura	service-template*		
DeleteServiceTemplateMinorVersion	Otorga permiso para eliminar una versión secundaria de la plantilla de servicio. OBSOLETO: utilícelo en su lugar DeleteServiceTemplateVersion	Escritura	service-template*		
DeleteServiceTemplateVersion	Otorga permiso para eliminar una versión de la plantilla de servicio	Escritura	service-template*		
DeleteTemplateSyncConfig	Otorga permiso para eliminar un TemplateSyncConfig	Escritura			
GetAccountRoles	Otorga permiso para obtener roles de cuenta. OBSOLETO: GetAccountSettings utilícelo en su lugar	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountSettings	Otorga permiso para describir la configuración de cuenta	Lectura			
GetComponent	Concede el permiso para describir un componente.	Lectura	component*		
GetDeployment	Concede permiso para describir una implementación	Lectura	deployment*		
GetEnvironment	Otorga permiso para describir un entorno.	Read	environment*		
GetEnvironmentAccountConnection	Otorga permiso para describir una conexión de cuenta de entorno	Read	environment-account-connection*		
GetEnvironmentTemplate	Otorga permiso para describir una plantilla de entorno.	Lectura	environment-template*		
GetEnvironmentTemplateMajorVersion	Otorga permiso para obtener una versión principal de la plantilla de entorno. OBSOLETO: utilícelo en su lugar GetEnvironmentTemplateVersion	Lectura	environment-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEnvironmentTemplateMinorVersion	Otorga permiso para obtener una versión secundaria de la plantilla de entorno. OBSOLETO: utilícelo en su lugar GetEnvironmentTemplateVersion	Lectura	environment-template*		
GetEnvironmentTemplateVersion	Otorga permiso para describir una versión de la plantilla de entorno	Lectura	environment-template*		
GetRepository	Otorga permiso para describir un repositorio	Lectura	repository*		
GetRepositorySyncStatus	Otorga permiso para obtener el estado de sincronización más reciente de un repositorio	Lectura			
GetResourceTemplateVersionStatusCounts	Otorga permiso para enumerar los recuentos de estado de las versiones de las plantillas de recursos	Lectura			
GetResourcesSummary	Otorga permiso para obtener el resumen de recursos	Lectura			
GetService	Otorga permiso para describir un servicio.	Read	service*		
GetServiceInstance	Otorga permiso para describir una instancia de servicio.	Lectura	service-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceInstanceSyncStatus	Concede permiso para describir el estado de sincronización de una instancia de servicio	Lectura			
GetServiceSyncBlockerSummary	Concede permiso para describir los bloqueadores de sincronización de servicio en un servicio o instancia de servicio	Lectura			
GetServiceSyncConfig	Concede permiso para describir una configuración de sincronización de servicio	Lectura			
GetServiceTemplate	Otorga permiso para describir una plantilla de servicio.	Lectura	service-template*		
GetServiceTemplateMajorVersion	Otorga permiso para obtener una versión principal de la plantilla de servicio. OBSOLETO: utilícelo en su lugar GetServiceTemplateVersion	Lectura	service-template*		
GetServiceTemplateMinorVersion	Otorga permiso para obtener una versión secundaria de la plantilla de servicio. OBSOLETO: utilícelo en su lugar GetServiceTemplateVersion	Lectura	service-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceTemplateVersion	Otorga permiso para describir una versión de la plantilla de servicio	Lectura	service-template*		
GetTemplateSyncConfig	Otorga permiso para describir un TemplateSyncConfig	Lectura			
GetTemplateSyncStatus	Otorga permiso para describir el estado de sincronización de una plantilla	Lectura			
ListComponentOutputs	Otorga permiso para enumerar las salidas de componentes	Enumeración	component*		
			deployment		
ListComponentProvisionedResources	Otorga permiso para mostrar una lista de los recursos aprovisionados de componentes.	Enumeración	component*		
ListComponents	Otorga permiso para enumerar componentes.	Enumeración	environment		
			service		
			service-instance		
ListDeployments	Otorga permiso para enumerar implementaciones	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEnvironmentAccountConnections	Otorga permiso para enumerar conexiones de cuenta de entorno	Enumeración			
ListEnvironmentOutputs	Otorga permiso para mostrar una lista de los resultados del entorno	Enumeración	environment* deployment		
ListEnvironmentProvisionedResources	Otorga permiso para mostrar una lista de los recursos aprovisionados del entorno	Enumeración	environment*		
ListEnvironmentTemplateMajorVersions	Otorga permiso para enumerar las versiones principales de la plantilla de entorno. OBSOLETO: ListEnvironmentTemplateVersions utilícelo en su lugar	Enumeración	environment-template*		
ListEnvironmentTemplateMinorVersions	Otorga permiso para enumerar las versiones secundarias de la plantilla de entorno. OBSOLETO: utilícelo en su lugar ListEnvironmentTemplateVersions	Enumeración	environment-template*		
ListEnvironmentTemplateVersions	Otorga permiso para enumerar las versiones de la plantilla de entorno	List	environment-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEnvironmentTemplates	Otorga permiso para enumerar las plantillas de entorno.	List			
ListEnvironments	Otorga permiso para enumerar los entornos.	Enumeración			
ListRepositories	Otorga permiso para enumerar repositorios	Enumeración			
ListRepositorySyncDefinitions	Otorga permiso para enumerar definiciones de sincronización de repositorios	Enumeración			
ListServiceInstanceOutputs	Otorga permiso para mostrar una lista de las salidas de las instancias de servicio	Enumeración	service*		
			service-instance*		
			deployment		
ListServiceInstanceProvisionedResources	Otorga permiso para mostrar una lista de los recursos aprovisionados de la instancia de servicio	Enumeración	service*		
			service-instance*		
ListServiceInstances	Otorga permiso para enumerar las instancias de servicio.	Enumeración			
		Enumeración	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServicePipelineOutputs	Otorga permiso para mostrar una lista de las salidas de la canalización de servicios		deployment		
ListServicePipelineProvisionedResources	Otorga permiso para mostrar una lista de los recursos aprovisionados de la canalización de servicios	Enumeración	service*		
ListServiceTemplateMajorVersions	Otorga permiso para enumerar las versiones principales de la plantilla de servicio. OBSOLETO: utilícelo en su lugar ListServiceTemplateVersions	Enumeración	service-template*		
ListServiceTemplateMinorVersions	Otorga permiso para enumerar las versiones secundarias de la plantilla de servicio. OBSOLETO: utilícelo en su lugar ListServiceTemplateVersions	Enumeración	service-template*		
ListServiceTemplateVersions	Otorga permiso para enumerar las versiones de la plantilla de servicio	List	service-template*		
ListServiceTemplates	Otorga permiso para enumerar las plantillas de servicio	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServices	Otorga permiso para enumerar los servicios.	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso	Lectura	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
NotifyResourceDeploymentStatusChange	Otorga permiso para notificar a Proton de los cambios en el estado de la implementación de recursos	Escritura	environment		
			service-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RejectEnvironmentAccountConnection	Otorga permiso para rechazar una solicitud de conexión de cuenta de entorno desde otra cuenta de entorno	Escritura	environment-account-connection*		
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccountRoles	Otorga permiso para actualizar roles de cuenta. OBSOLETO: utilícelo en su lugar UpdateAccountSettings	Escritura			iam:PassRole
UpdateAccountSettings	Otorga permiso para actualizar la configuración de cuenta	Escritura			iam:PassRole
UpdateComponent	Otorga permiso para actualizar componentes.	Escritura	component*		
UpdateEnvironment	Otorga permiso para actualizar un entorno.	Write	environment*		iam:PassRole
				proton:EnvironmentTemplate	
UpdateEnvironmentAccountConnection	Otorga permiso para actualizar una conexión de cuenta de entorno	Write	environment-account-connection*		
UpdateEnvironmentTemplate	Otorga permiso para actualizar una plantilla de entorno.	Escritura	environment-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateEnvironmentTemplateMajorVersion	Otorga permiso para actualizar una versión principal de la plantilla de entorno. OBSOLETO: utilícelo en su lugar UpdateEnvironmentTemplateVersion	Escritura	environment-template*		
UpdateEnvironmentTemplateMinorVersion	Otorga permiso para actualizar una versión secundaria de la plantilla de entorno. OBSOLETO: utilícelo en su lugar UpdateEnvironmentTemplateVersion	Escritura	environment-template*		
UpdateEnvironmentTemplateVersion	Otorga permiso para actualizar una versión de la plantilla de entorno	Write	environment-template*		
UpdateService	Otorga permiso para actualizar un servicio.	Write	service*		
				proton:ServiceTemplate	
UpdateServiceInstance	Otorga permiso para actualizar una instancia de servicio.	Write	service-instance*		
				proton:ServiceTemplate	
UpdateServicePipeline	Otorga permiso para actualizar una canalización de servicio.	Escritura	service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				proton:ServiceTemplate	
UpdateServiceSyncBlocker	Concede permiso para actualizar un bloqueador de sincronización de servicio	Escritura			
UpdateServiceSyncConfig	Concede permiso para actualizar una configuración de sincronización de servicio	Escritura			
UpdateServiceTemplate	Otorga permiso para actualizar una plantilla de servicio.	Escritura	service-template*		
UpdateServiceTemplateMajorVersion	Otorga permiso para actualizar una versión principal de la plantilla de servicio. OBSOLETO: utilícelo en su lugar UpdateServiceTemplateVersion	Escritura	service-template*		
UpdateServiceTemplateMinorVersion	Otorga permiso para crear una versión secundaria de la plantilla de servicio. OBSOLETO: utilícelo en su lugar UpdateServiceTemplateVersion	Escritura	service-template*		
UpdateServiceTemplateVersion	Otorga permiso para actualizar una versión de la plantilla de servicio	Escritura	service-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTemplateSyncConfig	Otorga permiso para actualizar un TemplateSyncConfig	Escritura			

Tipos de recursos definidos por AWS Proton

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment-template	`arn:${Partition}:proton:${Region}:${Account}:environment-template/${Name}`	aws:ResourceTag/${TagKey}
environment-template-version	`arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersion}.${MinorVersion}`	aws:ResourceTag/${TagKey}
environment-template-major-version	`arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}`	aws:ResourceTag/${TagKey}
environment-template-minor-version	`arn:${Partition}:proton:${Region}:${Account}:environment-template/${Temp`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
	lateName}:${MajorVersionId}.${MinorVersionId}	
service-template	arn:${Partition}:proton:${Region}:${Account}:service-template/${Name}	aws:ResourceTag/${TagKey}
service-template-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
service-template-major-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
service-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
environment	arn:${Partition}:proton:${Region}:${Account}:environment/${Name}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:proton:${Region}:${Account}:service/${Name}	aws:ResourceTag/${TagKey}
service-instance	arn:${Partition}:proton:${Region}:${Account}:service/${ServiceName}/service-instance/${Name}	aws:ResourceTag/${TagKey}
environment-account-connection	arn:${Partition}:proton:${Region}:${Account}:environment-account-connection/${Id}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
repository	`arn:${Partition}:proton:${Region}:${Account}:repository/${Provider}:${Name}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:proton:${Region}:${Account}:component/${Id}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:proton:${Region}:${Account}:deployment/${Id}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Proton

AWS Proton define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
proton:EnvironmentTemplate	Filtra el acceso según la plantilla de entorno especificada y relacionada con el recurso.	Cadena
proton:ServiceTemplate	Filtra el acceso según la plantilla de servicio especificada y relacionada con el recurso.	Cadena

Acciones, recursos y claves de condición para AWS Purchase Orders Console

AWS La consola de pedidos de compra (prefijo de servicio:`purchase-orders`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Purchase Orders Console
- Tipos de recursos definidos por AWS Purchase Orders Console
- Claves de condición para AWS Purchase Orders Console

Acciones definidas por AWS Purchase Orders Console

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddPurchaseOrder [solo permiso]	Concede permiso para agregar una nueva orden de compra	Escritura	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [solo permiso]	Concede permiso para eliminar una orden de compra	Escritura	purchase-order*		
				aws:ResourceTag/${TagKey}	
GetConsoleActionSetEnforced [solo permiso]	Concede permiso para ver si se utilizan acciones de IAM existentes o detalladas para controlar la autorización en las consolas de facturación, administración de costos y cuenta	Lectura			
GetPurchaseOrder [solo permiso]	Concede permiso para obtener una orden de compra	Lectura	purchase-order*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPurchaseOrderInvoices [solo permiso]	Concede permiso para enumerar facturas de órdenes de compra	Enumeración	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrders [solo permiso]	Concede permiso para enumerar todos los pedidos de compra de una cuenta	Enumeración			
ListTagsForResource [solo permiso]	Concede permiso para enumerar un pedido de compra	Lectura	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders [solo permiso]	Concede permiso para modificar las órdenes de compra y los detalles	Escritura	purchase-order*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource [solo permiso]	Concede permiso para etiquetar órdenes de compra con pares de valores de clave dados	Etiquetado	purchase-order*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [solo permiso]	Concede permiso para eliminar etiquetas de una orden de compra	Etiquetado	purchase-order*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [solo permiso]	Concede permiso para cambiar si se utilizarán acciones de IAM existentes o detalladas para controlar la autorización en las consolas de facturación, administración de costos y cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePurchaseOrder [solo permiso]	Concede permiso para actualizar una orden de compra existente	Escritura	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus [solo permiso]	Concede permiso para establecer el estado de una orden de compra	Escritura	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders [solo permiso]	Concede permiso para ver las órdenes de compra y los detalles	Lectura	purchase-order		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS Purchase Orders Console

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
purchase-order	`arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Purchase Orders Console

AWS La consola de pedidos de compra define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante los pares clave-valor de etiqueta adjuntados al recurso.	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Q

Amazon Q (prefijo de servicio: q) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Q
- Tipos de recurso definidos por Amazon Q
- Claves de condición de Amazon Q

Acciones definidas por Amazon Q

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate Connector Resource [solo permiso]	Otorga permiso para asociar un AWS recurso a un conector Amazon Q	Escritura			
CreateAssignment [solo permiso]	Concede permiso para crear una asignación de usuario o grupo para un perfil de Amazon Q Developer	Escritura	profile*		
				identitystore:UserId identitystore:GroupId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAuthGrant [solo permiso]	Otorga permiso para crear un OAuth usuario en Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreateOAuthAppConnection [solo permiso]	Otorga permiso para registrar una OAuth aplicación en Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreatePlugin [solo permiso]	Otorga permiso para crear y configurar un complemento de terceros en Amazon Q	Escritura	plugin*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAssignment [solo permiso]	Concede permiso para eliminar una asignación de usuario o grupo para un perfil de Amazon Q Developer	Escritura	profile*		
				identitystore:UserId identitystore:GroupId	
DeleteConversation [solo permiso]	Otorga permiso para eliminar una conversación con Amazon Q	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteOAuthAppConnection [solo permiso]	Otorga permiso para eliminar una OAuth aplicación en Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
DeletePlugin [solo permiso]	Otorga permiso para eliminar un complemento configurado en Amazon Q	Escritura	plugin*		
				aws:ResourceTag/${TagKey}	
GenerateCodeFromCommands [solo permiso]	Concede permiso para generar código a partir de comandos CLI en Amazon Q	Lectura			
GenerateCodeRecommendations [solo permiso]	Otorga permiso para generar recomendaciones de código en Amazon Q	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnector [solo permiso]	Otorga permiso para ver información sobre un conector Amazon Q específico	Lectura			
GetConversation [solo permiso]	Concede permiso para obtener mensajes individuales asociados a una conversación específica con Amazon Q	Lectura			
GetIdentityMetadata [solo permiso]	Concede permiso a Amazon Q para obtener los metadatos de identidad	Lectura			
GetPlugin [solo permiso]	Otorga permiso para ver información sobre un complemento de Amazon Q configurado específico	Lectura	plugin*		
				aws:ResourceTag/${TagKey}	
GetTroubleshootingResults [solo permiso]	Concede permiso para obtener resultados de solución de problemas con Amazon Q	Lectura			
ListConversations [solo permiso]	Concede permiso para enumerar las conversaciones individuales asociadas a un usuario específico de Amazon Q	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDashboardMetrics [solo permiso]	Otorga permiso para leer las métricas y rellenar el panel de control de Amazon Q	Enumeración			
ListPluginProviders [solo permiso]	Otorga permiso para publicar los complementos disponibles en Amazon Q	Enumeración			
ListPlugins [solo permiso]	Otorga permiso para enumerar los complementos configurados en Amazon Q	Enumeración	plugin*		
ListTagsForResource [solo permiso]	Otorga permiso para enumerar todas las etiquetas asociadas a un recurso de Amazon Q	Enumeración	plugin		
				aws:ResourceTag/${TagKey}	
PassRequest [solo permiso]	Concede permiso para permitir que Amazon Q realice acciones en su nombre	Escritura			
RejectConnector [solo permiso]	Concede permiso para rechazar una solicitud de conexión para un conector Amazon Q	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendEvent [solo permiso]	Otorga permiso para activar acciones asíncronas de Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
SendMessage [solo permiso]	Concede permiso para enviar un mensaje a Amazon Q	Escritura			
StartConversation [solo permiso]	Concede permiso para iniciar una conversación con Amazon Q	Escritura			
StartTroubleshootingAnalysis [solo permiso]	Concede permiso para iniciar un análisis de solución de problemas con Amazon Q	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartTroubleshootingResolutionExplanation [solo permiso]	Concede permiso para comenzar una explicación de resolución de problemas con Amazon Q	Escritura			
TagResource [solo permiso]	Otorga permiso para asociar etiquetas a un recurso de Amazon Q	Etiquetado	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [solo permiso]	Otorga permiso para eliminar las etiquetas asociadas a un recurso de Amazon Q	Etiquetado	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAuthGrant [solo permiso]	Otorga permiso para actualizar OAuth el usuario en Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdateConversation [solo permiso]	Otorga permiso para actualizar una conversación con Amazon Q	Escritura			
UpdateOAuthAppConnection [solo permiso]	Otorga permiso para actualizar una OAuth aplicación en Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdatePlugin [solo permiso]	Otorga permiso para actualizar un complemento de terceros en Amazon Q	Escritura	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTroubleshootingCommandResult [solo permiso]	Concede permiso para actualizar el resultado de un comando de solución de problemas con Amazon Q	Escritura			
UsePlugin [solo permiso]	Otorga permiso para usar los complementos de Amazon Q	Escritura	plugin*		
VerifyOAuthAppConnection [solo permiso]	Otorga permiso para verificar una OAuth aplicación en Amazon Q	Escritura			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Tipos de recurso definidos por Amazon Q

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	
plugin	`arn:${Partition}:qdeveloper:${Region}:${Account}:plugin/${Identifier}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Q

Amazon Q define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso Amazon Q	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
identitystore:GroupId	Filtra el acceso por el ID del grupo de IAM Identity Center	ArrayOfString
identitystore:UserId	Filtra el acceso por ID de usuario de IAM Identity Center	ArrayOfString

Acciones, recursos y claves de condición para Amazon Q Business

Amazon Q Business (prefijo de servicio: `qbusiness`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Q Business
- Tipos de recursos definidos por Amazon Q Business
- Claves de condición de Amazon Q Business

Acciones definidas por Amazon Q Business

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddUserLicenses	Concede permiso para agregar uno o varios usuarios para las licencias	Escritura			
AllowVendedLogDeliveryForResource [solo permiso]	Concede permiso para configurar la entrega de registros suministrados para el recurso de la aplicación de Amazon Q Business	Administración de permisos	application*		
				aws:ResourceTag/${TagKey}	
AssociatePermission	Otorga permiso para asociar la declaración de política basada en los recursos a la aplicación	Escritura	application*		qbusiness:PutResourcePolicy
BatchDeleteDocument	Concede permiso para documento de eliminación por lotes	Escritura	application*		
			index*		
BatchPutDocument	Concede permiso para documento de inserción por lotes	Escritura	application*		
			index*		
CancelSubscription	Concede permiso para cancelar una suscripción	Escritura	application*		
			subscription*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Chat	Concede permiso para chatear mediante una aplicación	Lectura	application*		
ChatSync	Concede permiso para chatear de forma sincrónica mediante una aplicación	Lectura	application*		
CheckDocumentAccess	Otorga permiso para comprobar si un usuario tiene acceso a un documento	Lectura	application*		
			index*		
CreateAnonymousWebExperienceUrl	Otorga permiso para crear una URL única para una experiencia web anónima de Amazon Q Business	Escritura	application*		
			web-experience*		
CreateApplication	Concede permiso para crear una aplicación.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateChatResponseConfiguration	Otorga permiso para crear una configuración de respuesta de chat a la aplicación	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessor	Otorga permiso de creación DataAccessor a la aplicación	Escritura	application*		qbusiness:CreateDataAccessorWithTti
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessorWithTti [solo permiso]	Otorga permiso para crear un emisor de token de confianza del centro de identidad de AWS IAM en función de DataAccessor la aplicación	Escritura	application*		
CreateDataSource	Concede permiso para crear un origen de datos para un índice y una aplicación determinados	Escritura	application*		
			index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Concede permiso para crear una instantánea para una aplicación determinada	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegration	Otorga permiso para crear una nueva integración para una aplicación de Q Business	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicense	Concede permiso para crear una licencia	Escritura			
CreatePlugin	Concede permiso para crear un complemento para una aplicación determinada	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetriever	Concede permiso para crear un recuperador para una aplicación determinada	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Concede permiso para crear una suscripción	Escritura	application*		
				identitystore:UserId identitystore:GroupId	
CreateUser	Concede permiso para crear un usuario	Escritura	application*		
CreateWebExperience	Concede permiso para crear una experiencia web para una aplicación determinada	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permiso para eliminar una aplicación.	Escritura	application*		
DeleteAttachment	Otorga permiso para eliminar un archivo adjunto en el contexto de chat actual	Escritura	application*		
DeleteChatControlsConfiguration	Concede permiso para eliminar la configuración de los controles del chat para una aplicación	Escritura	application*		
DeleteChatResponseConfiguration	Otorga permiso para eliminar una configuración de respuesta de chat	Escritura	application*		
			chat-response-configuration*		
DeleteConversation	Concede permiso para eliminar una conversación	Escritura	application*		
DeleteDataAccessor	Otorga permiso para eliminar DataAccessor	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			data-accessor*		
DeleteDataSource	Otorga permiso para eliminar un DataSource	Escritura	application*		
			data-source*		
			index*		
DeleteGroup	Concede permiso para eliminar un grupo	Escritura	application*		
			index*		
DeleteIndex	Concede permiso para eliminar un índice	Escritura	application*		
			index*		
DeleteIntegration	Otorga permiso para eliminar una integración de una aplicación de Q Business	Escritura	application*		
			integration*		
DeletePlugin	Concede permiso para eliminar un complemento	Escritura	application*		
			plugin*		
DeleteRetriever	Concede permiso para eliminar un recuperador	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			retriever*		
DeleteUser	Concede permiso para eliminar un usuario	Escritura	application*		
DeleteWebExperience	Concede permiso para eliminar una experiencia web	Escritura	application*		
			web-experience*		
DisableAclOnDataSource [solo permiso]	Concede permiso para desactivar el rastreo de ACL al crear el recurso de origen de datos de Amazon Q Business	Escritura	application*		
DisassociatePermission	Otorga permiso para disociar la declaración de política basada en recursos de la aplicación	Escritura	application*		qbusiness:PutResourcePolicy
GetApplication	Concede el permiso para obtener una aplicación	Lectura	application*		
GetChatControlsConfiguration	Concede permiso para obtener la configuración de los controles de chat de una aplicación	Enumeración	application*		
GetChatResponseConfiguration	Otorga permiso para obtener una configuración de respuesta de chat	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			chat-response-configuration*		
GetDataAccessor	Otorga permiso para obtener DataAccessor	Lectura	application*		
			data-accessor*		
GetDataSource	Concede permiso para obtener un origen de datos	Lectura	application*		
			data-source*		
			index*		
GetGroup	Concede permiso para obtener un grupo	Lectura	application*		
			index*		
GetIndex	Concede permiso para obtener un índice	Lectura	application*		
			index*		
GetIntegration	Otorga permiso para obtener una integración para una aplicación de Q Business	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			integration*		
GetLicense	Otorga permiso para obtener una licencia.	Lectura	user-license*		
GetMedia	Otorga permiso para asociar el contenido multimedia a un mensaje del sistema	Lectura	application*		
GetPlugin	Concede permiso para obtener un complemento	Lectura	application*		
			plugin*		
GetPolicy	Otorga permiso para obtener la política de la aplicación basada en los recursos	Lectura	application*		
GetRetriever	Concede permiso para obtener un recuperador	Lectura	application*		
			retriever*		
GetUser	Concede permiso para obtener un usuario	Lectura	application*		
GetWebExperience	Concede permiso para obtener una experiencia web	Lectura	application*		
			web-experience*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApplications	Concede permiso para enumerar las aplicaciones	Enumeración			
ListAttachments	Otorga permiso para enumerar los archivos adjuntos en el contexto de chat actual	Enumeración	application*		
ListChatResponseConfigurations	Otorga permiso para enumerar las configuraciones de respuesta de chat de una aplicación	Enumeración	application*		
ListConversations	Concede permiso para enumerar todas las conversaciones para una aplicación	Enumeración	application*		
ListDataAccessors	Otorga permiso DataAccessors para incluir listas en la aplicación	Enumeración	application*		
ListDataSourceSyncJobs	Concede permiso para obtener el historial de trabajos de sincronización de orígenes de datos	Enumeración	application*		
			data-source*		
			index*		
ListDataSources	Concede permiso para enumerar los orígenes de datos de una aplicación y un índice	Enumeración	application*		
			index*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDocuments	Concede permiso para enumerar todos los documentos	Enumeración	application*		
			index*		
ListGroups	Concede permiso para enumerar los grupos	Enumeración	application*		
			index*		
ListIndices	Concede permiso para enumerar los índices de una aplicación	Enumeración	application*		
ListIntegrations	Otorga permiso para enumerar todas las integraciones de una aplicación de Q Business	Enumeración	application*		
ListMessages	Concede permiso para enumerar todos los mensajes	Enumeración	application*		
ListPluginActions	Otorga permiso para enumerar las acciones de un complemento dentro de la aplicación	Lectura	application*		
			plugin*		
ListPluginTypeActions	Otorga permiso para enumerar todas las acciones de un tipo de complemento	Lectura			
ListPluginTypeMetadata	Otorga permiso para enumerar todos los metadatos del tipo de complemento	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPlugins	Concede permiso para enumerar los complementos de una aplicación	Enumeración	application*		
ListRetrievers	Concede permiso para enumerar los recuperadores de una aplicación	Enumeración	application*		
ListSubscriptions	Concede permiso para enumerar suscripciones	Enumeración	application*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			web-experience		
ListUserLicenses	Concede permiso para enumerar las licencias.	Enumeración			
ListWebExperiences	Concede permiso para enumerar las experiencias web de una aplicación	Enumeración	application*		
PutFeedback	Concede permiso para enviar comentarios sobre un mensaje de conversación	Escritura	application*		
PutGroup	Concede los permisos para poner un grupo de usuarios	Escritura	application*		
			index*		
PutResourcePolicy [solo permiso]	Otorga permiso para incluir en la aplicación una declaración de política basada en recursos	Escritura	application*		
RemoveUserLicenses	Concede permiso para eliminar licencias para uno o varios usuarios	Escritura			
SearchRelevantContent	Otorga permiso para buscar contenido relevante en la aplicación Amazon Q Business	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDataSourceSyncJob	Otorga permiso para iniciar el trabajo de sincronización de orígenes de datos	Escritura	application*		
			data-source*		
			index*		
StartDeployment	Otorga permiso para iniciar la implementación de una integración	Escritura	application*		
			integration*		
StopDataSourceSyncJob	Otorga permiso para detener el trabajo de sincronización de orígenes de datos	Escritura	application*		
			data-source*		
			index*		
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	application		
			chat-response-configuration		
			data-accessor		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar de un recurso la etiqueta con la clave dada	Etiquetado	application		
			chat-response-configuration		
			data-accessor		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
				aws:TagKeys	
UpdateApplication	Concede permiso para actualizar una aplicación	Escritura	application*		
UpdateChatControlsConfiguration	Concede permiso para actualizar una configuración del controles de chat para una aplicación	Escritura	application*		
UpdateChatResponseConfiguration	Otorga permiso para actualizar la configuración de una respuesta de chat	Escritura	application*		
			chat-response-configuration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDataAccessor	Otorga permiso para actualizar DataAccessor	Escritura	application*		
			data-accessor*		
UpdateDataSource	Otorga permiso para actualizar un DataSource	Escritura	application*		
			data-source*		
			index*		
UpdateIndex	Concede permiso para actualizar un índice	Escritura	application*		
			index*		
UpdateIntegration	Otorga permiso para actualizar una integración de una aplicación de Q Business	Escritura	application*		
			integration*		
UpdatePlugin	Concede permiso para actualizar un complemento	Escritura	application*		
			plugin*		
UpdateRetriever	Concede permisos para actualizar un recuperador	Escritura	application*		
			retriever*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSubscription	Concede permiso para actualizar una suscripción	Escritura	application*		
			subscription*		
UpdateUser	Concede permisos para actualizar un usuario	Escritura	application*		
UpdateWebExperience	Otorga permiso para actualizar un WebExperience	Escritura	application*		
			web-experience*		

Tipos de recursos definidos por Amazon Q Business

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
integration	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/integration/${IntegrationId}	aws:ResourceTag/${TagKey}
retriever	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/retriever/${RetrieverId}	aws:ResourceTag/${TagKey}
index	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}	aws:ResourceTag/${TagKey}
data-source	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}/data-source/${DataSourceId}	aws:ResourceTag/${TagKey}
plugin	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/plugin/${PluginId}	aws:ResourceTag/${TagKey}
web-experience	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/web-experience/${WebExperienceId}	aws:ResourceTag/${TagKey}
user-license	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/user-license/${UserLicenseId}	
subscription	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/subscription/${SubscriptionId}	

Tipos de recurso	ARN	Claves de condición
data-accessor	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/data-accessor/${DataAccessorId}`	aws:ResourceTag/${TagKey}
chat-response-configuration	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/chat-response-configuration/${ChatResponseConfigurationId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Q Business

Amazon Q Business define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
identitystore:GroupId	Filtra el acceso por el ID del grupo de IAM Identity Center	ArrayOfString

Claves de condición	Descripción	Tipo
identitystore:UserId	Filtra el acceso por ID de usuario de IAM Identity Center	ArrayOfString

Acciones, recursos y claves de condición para las aplicaciones de Q de Amazon Q Business

Aplicaciones de Q de Amazon Q Business (prefijo del servicio: `qapps`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las aplicaciones de Q de Amazon Q Business
- Tipos de recursos definidos por las aplicaciones de Q de Amazon Q Business
- Claves de condición para las aplicaciones de Q de Amazon Q Business

Acciones definidas por las aplicaciones de Q de Amazon Q Business

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateLibraryItemReview	Concede permiso para asociar una revisión de un elemento de la biblioteca en el entorno de la aplicación Q de Amazon Q Business	Escritura	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
AssociateQAppWithUser	Concede permiso para asociar una aplicación de Q de Amazon Q Business a un usuario en el entorno de la aplicación Q de Amazon Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
BatchCreateCategory	Otorga permiso para crear las categorías de una biblioteca en el entorno de aplicaciones de Q Business	Escritura	application*		
BatchDeleteCategory	Otorga permiso para eliminar las categorías de una biblioteca en el entorno de aplicaciones de Q Business	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchUpdateCategory	Otorga permiso para actualizar las categorías de una biblioteca en el entorno de aplicaciones de Q Business	Escritura	application*		
CopyQApp [solo permiso]	Concede permiso para copiar la aplicación de Q en el entorno de la aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItem	Concede permiso para crear un elemento de biblioteca en el entorno de aplicación de Q Business.	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateLibraryItemReview [solo permiso]	Concede permiso para crear una revisión de un elemento de biblioteca en el entorno de aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateQApp	Concede permiso para crear una aplicación de Q en el entorno de aplicación de Q Business	Escritura	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionToken [solo permiso]	Concede permiso para suscribirse a un tema del bus de eventos de una aplicación de Q en el entorno de aplicación de Q Business	Escritura	application*		
DeleteLibraryItem	Concede permiso para eliminar un elemento de biblioteca en el entorno de aplicación de Q Business	Escritura	application		
			qapp		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				qapps:UserIsAppOwner qapps:AppIsPublished	
DeleteQApp	Concede permiso para eliminar una aplicación de Q en el entorno de aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DescribeQAppPermissions	Otorga permiso para obtener permisos de uso compartido de Q App en el entorno de aplicaciones de Q Business	Lectura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateLibraryItemReview	Concede permiso para desasociar una revisión de un elemento de biblioteca en el entorno de aplicación de Q Business	Escritura	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateQAppFromUser	Concede permiso para desasociar una aplicación de Q con un usuario en el entorno de aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
ExportQAppSessionData	Concede permiso para exportar datos de sesión de la aplicación de Q en el entorno de aplicación de Q Business	Escritura	qapp-session*		
GetLibraryItem	Concede permiso para obtener un elemento de biblioteca en el entorno de aplicación de Q Business	Lectura	application		
			qapp		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQApp	Concede permiso para obtener la aplicación de Q en el entorno de aplicación de Q Business	Lectura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQAppSession	Concede permiso para obtener la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Lectura	qapp-session*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
GetQAppSessionMetadata	Concede permiso para obtener los metadatos de la sesión de una aplicación de Q en el entorno de aplicación de Q Business	Lectura	qapp-session*		
ImportDocument	Concede permiso para importar un documento a la aplicación de Q o a la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Escritura	qapp		
			qapp-session		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
ListCategories	Otorga permiso para enumerar categorías en el entorno de aplicaciones de Q Business	Enumeración	application*		
ListLibraryItems	Concede permiso para enumerar elementos de biblioteca en el entorno de aplicación de Q Business	Enumeración	application*		
ListQAppSessionData	Concede permiso para obtener los datos de la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Lectura	qapp-session*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQApps	Concede permiso para enumerar aplicaciones de Q en el entorno de aplicación de Q Business	Enumeración	application*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	qapp		
			qapp-session		
PredictProblemStatementFromConversation [solo permiso]	Concede permiso para predecir una declaración de problema a partir del registro de conversación en el entorno de aplicación de Q Business	Escritura	application*		
PredictQApp	Concede permiso para predecir la aplicación de Q a partir del registro de conversación o de la declaración de problema en el entorno de aplicación de Q Business	Escritura	application*		
PredictQAppFromProblemStatement [solo permiso]	Concede permiso para predecir los metadatos de la aplicación de Q a partir de la declaración de problema en el entorno de aplicación de Q Business	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartQAppSession	Concede permiso para iniciar la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished aws:RequestTag/${TagKey} aws:TagKeys	
StopQAppSession	Concede permiso para detener la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Escritura	application		
			qapp-session		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	qapp		
			qapp-session		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar de un recurso la etiqueta con la clave dada	Etiquetado	qapp		
			qapp-session		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateLibraryItem	Concede permiso para actualizar un elemento de biblioteca en el entorno de aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateLibraryItemMetadata	Concede permiso para actualizar los metadatos de un elemento de biblioteca en el entorno de aplicación de Q Business	Escritura	qapp*		
				qapps:AppIsPublished	
UpdateQApp	Concede permiso para actualizar la aplicación de Q en el entorno de aplicación de Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQAppPermissions	Otorga permiso para actualizar los permisos de uso compartido de Q App en el entorno de aplicaciones Q Business	Escritura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateQAppSession	Concede permiso para actualizar la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Escritura	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQAppSessionMetadata	Concede permiso para actualizar los metadatos de la sesión de la aplicación de Q en el entorno de aplicación de Q Business	Escritura	qapp-session*		

Tipos de recursos definidos por las aplicaciones de Q de Amazon Q Business

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	
qapp	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}`	aws:ResourceTag/${TagKey}
qapp-session	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}/session/${SessionId}`	aws:ResourceTag/${TagKey}

Claves de condición para las aplicaciones de Q de Amazon Q Business

Las aplicaciones de Q de Amazon Q Business definen las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
qapps:AppIsPublished	Filtra el acceso en función de si la aplicación de Q está publicada	Cadena
qapps:SessionIsShared	Filtra el acceso según si la sesión de la aplicación de Q se ha compartido	Cadena
qapps:UserIsAppOwner	Filtra el acceso según si el solicitante es propietario de la aplicación de Q	Cadena
qapps:UserIsSessionModerator	Filtra el acceso según si el solicitante es moderador de la sesión de la aplicación de Q	Cadena

Acciones, recursos y claves de condición para Amazon Q Developer

Amazon Q Developer (prefijo de servicio:`qdeveloper`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el desarrollador de Amazon Q
- Tipos de recursos definidos por Amazon Q Developer
- Claves de condición para Amazon Q Developer

Acciones definidas por el desarrollador de Amazon Q

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExportArtifact	Concede permiso para exportar artefactos del desarrollador de Amazon Q	Escritura	codeTransformation		
ImportArtifact	Otorga permiso para importar artefactos a Amazon Q Developer	Escritura	codeTransformation		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource [solo permiso]	Otorga permiso para enumerar todas las etiquetas asociadas a un recurso para desarrolladores de Amazon Q	Enumeración	codeTransformation		
StartAgentSession	Otorga permiso para iniciar una sesión de agente con Amazon Q Developer	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [solo permiso]	Otorga permiso para asociar etiquetas a un recurso para desarrolladores de Amazon Q	Etiquetado	codeTransformation		
				aws:TagKeys aws:RequestTag/${TagKey}	
TransformCode	Otorga permiso para transformar código con Amazon Q Developer Transform Agent	Escritura	codeTransformation		
UntagResource [solo permiso]	Otorga permiso para eliminar las etiquetas asociadas a un recurso para desarrolladores de Amazon Q	Etiquetado	codeTransformation		
				aws:TagKeys	

Tipos de recursos definidos por Amazon Q Developer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
codeTransformation	`arn:${Partition}:qdeveloper:${Region}:${Account}:codeTransformation/${Identifier}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Q Developer

El desarrollador de Amazon Q define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso Amazon Q Developer	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Q in Connect

Amazon Q in Connect (prefijo de servicio: `wisdom`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Q in Connect
- Tipos de recurso definidos por Amazon Q in Connect
- Claves de condición de Amazon Q in Connect

Acciones definidas por Amazon Q in Connect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateMessageTemplate	Concede permiso para activar una plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
AllowVendedLogDeliveryForResource [solo permiso]	Concede permiso para configurar la entrega de registros suministrados para un asistente	Administración de permisos	Assistant		
CreateAIAgent	Concede permiso para crear un agente de IA	Escritura	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIAgentVersion	Concede permiso para crear una versión de un agente de IA	Escritura	AIAgent*		
			Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAIGuardrail	Otorga permiso para crear una barandilla de aire	Escritura	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrailVersion	Otorga permiso para crear una versión de barandilla aérea	Escritura	AIGuardrail*		
			Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPrompt	Concede permiso para crear una petición de IA	Escritura	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPromptVersion		Escritura	AIPrompt*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para crear una versión de una petición de IA		Assistant *		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistant	Otorga permiso para crear un asistente	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistantAssociation	Otorga permiso para crear una asociación entre un asistente y otro recurso	Escritura	Assistant *		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContent	Otorga permiso para crear contenido	Escritura	KnowledgeBase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContentAssociation	Concede permiso para crear una asociación de contenido	Escritura	Content*		
			KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKnowledgeBase	Concede permiso para crear una base de conocimientos	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplate	Concede permiso para crear una plantilla de mensaje	Escritura	KnowledgeBase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplateAttachment	Concede permiso para crear un archivo adjunto a una plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
CreateMessageTemplateVersion	Concede permiso para crear una versión de una plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
CreateQuickResponse	Otorga permiso para crear una respuesta rápida	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSession	Concede permiso para crear una sesión	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeactivateMessageTemplate	Concede permiso para desactivar una plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
DeleteAIAgent	Concede permiso para eliminar un agente de IA	Escritura	AIAgent*		
			Assistant*		
DeleteAIAgentVersion	Concede permiso para eliminar una versión de un agente de IA	Escritura	AIAgent*		
			Assistant*		
DeleteAIGuardrail	Otorga permiso para eliminar una barandilla aérea	Escritura	AIGuardrail*		
			Assistant*		
DeleteAIGuardrailVersion	Otorga permiso para eliminar una versión de barandilla aérea	Escritura	AIGuardrail*		
			Assistant*		
DeleteAIPrompt	Concede permiso para eliminar una petición de IA	Escritura	AIPrompt*		
			Assistant*		
DeleteAIPromptVersion		Escritura	AIPrompt*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para eliminar una versión de una petición de IA		Assistant*		
DeleteAssistant	Otorga permiso para eliminar un asistente	Escritura	Assistant*		
DeleteAssistantAssociation	Otorga permiso para eliminar una asociación con el asistente	Escritura	Assistant*		
			AssistantAssociation*		
DeleteContent	Otorga permiso para eliminar contenido	Escritura	Content*		
			KnowledgeBase*		
DeleteContentAssociation	Concede permiso para eliminar una asociación de contenido	Escritura	Content*		
			ContentAssociation*		
			KnowledgeBase*		
DeleteImportJob	Concede permiso para eliminar un trabajo importante de una base de conocimientos	Escritura	KnowledgeBase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteKnowledgeBase	Concede permiso para eliminar una base de conocimientos	Escritura	KnowledgeBase*		
DeleteMessageTemplate	Concede permiso para eliminar una plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
DeleteMessageTemplateAttachment	Concede permiso para eliminar un archivo adjunto de una plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
DeleteQuickResponse	Otorga permiso para eliminar una respuesta rápida	Escritura	KnowledgeBase*		
			QuickResponse*		
GetAIAgent	Concede permiso para recuperar información sobre un agente de IA	Lectura	AIAgent*		
			Assistant*		
GetAIGuardrail	Otorga permiso para recuperar información sobre una barandilla aérea	Lectura	AIGuardrail*		
			Assistant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAIPrompt	Concede permiso para recuperar información sobre una petición de IA	Lectura	AIPrompt*		
			Assistant*		
GetAssistant	Otorga permiso para recuperar información acerca del asistente	Lectura	Assistant*		
GetAssistantAssociation	Otorga permiso para recuperar información acerca de la asociación con el asistente	Lectura	Assistant*		
			AssistantAssociation*		
GetContent	Otorga permiso para recuperar contenido, incluida una dirección URL prefirmada para descargar el contenido	Lectura	Content*		
			KnowledgeBase*		
GetContentAssociation	Concede permiso para recuperar información sobre una asociación de contenido	Lectura	Content*		
			ContentAssociation*		
			KnowledgeBase*		
GetContentSummary	Otorga permiso para recuperar información resumida sobre el contenido	Lectura	Content*		
			KnowledgeBase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetImportJob	Otorga permiso para recuperar información acerca de un trabajo importante.	Lectura	KnowledgeBase*		
GetKnowledgeBase	Otorga permiso para recuperar información acerca de la base de conocimientos	Lectura	KnowledgeBase*		
GetMessageTemplate	Concede permiso para recuperar una plantilla de mensaje	Lectura	KnowledgeBase*		
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
GetNextMessage	Otorga permiso para recuperarla para el siguiente mensaje de una sesión	Lectura	Assistant*		
			Session*		
GetQuickResponse	Concede permiso para recuperar contenido.	Lectura	KnowledgeBase*		
			QuickResponse*		
GetRecommendations	Otorga permiso para recuperar recomendaciones para la sesión especificada	Lectura	Assistant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSession	Otorga permiso para recuperar información para una sesión especificada	Lectura	Assistant*		
			Session*		
ListAIAgentVersions	Concede permiso para enumerar información sobre versiones del agente de IA	Enumeración	AIAgent*		
			Assistant*		
ListAIAgents	Concede permiso para enumerar información sobre agentes de IA	Enumeración	Assistant*		
ListAIGuardrailVersions	Otorga permiso para incluir información sobre las versiones de ai guardrail	Enumeración	AIGuardrail*		
			Assistant*		
ListAIGuardrails	Otorga permiso para incluir información sobre las barandillas aéreas	Enumeración	Assistant*		
ListAIPromptVersions	Concede permiso para enumerar información sobre versiones de una petición de IA	Enumeración	AIPrompt*		
			Assistant*		
ListAIPrompts	Concede permiso para enumerar información sobre peticiones de IA	Enumeración	Assistant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAssistantAssociations	Otorga permiso para enumerar información acerca de la asociación con el asistente	Enumeración			
ListAssistants	Otorga permiso para enumerar información acerca de los asistentes	Enumeración			
ListContentAssociations	Concede permiso para enumerar información sobre asociaciones de contenido	Enumeración	Content*		
			KnowledgeBase*		
ListContents	Otorga permiso para enumerar el contenido con una base de conocimientos	Enumeración	KnowledgeBase*		
ListImportJobs	Otorga permiso para enumerar información acerca de la base de conocimientos	Enumeración	KnowledgeBase*		
ListKnowledgeBases	Otorga permiso para enumerar información acerca de la base de conocimientos	Enumeración			
ListMessageTemplateVersions	Concede permiso para enumerar versiones de plantilla de mensaje para la plantilla de mensaje especificada	Enumeración	KnowledgeBase*		
			MessageTemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMessageTemplates	Concede permiso para enumerar plantillas de mensaje para una base de conocimientos	Enumeración	KnowledgeBase*		
ListMessages	Otorga permiso para incluir los mensajes de una sesión	Enumeración	Assistant*		
			Session*		
ListQuickResponses	Otorga permiso para enumerar la respuesta rápida con una base de conocimientos	Enumeración	KnowledgeBase*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas del recurso especificado	Lectura			
NotifyRecommendationsReceived	Otorga permiso para eliminar las recomendaciones especificadas de la cola de recomendaciones nuevas disponibles del asistente especificado	Escritura			
PutFeedback	Concede permiso para enviar comentarios	Escritura	Assistant*		
QueryAssistant	Otorga permiso para realizar una búsqueda manual con el asistente especificado	Lectura	Assistant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveAssistantAIAgent	Concede permiso para quitar un agente de IA de un asistente	Escritura	Assistant*		
RemoveKnowledgeBaseTemplateUri	Otorga permiso para quitar una plantilla URI de una base de conocimientos	Escritura	KnowledgeBase*		
RenderMessageTemplate	Concede permiso para renderizar una plantilla de mensaje	Lectura	KnowledgeBase*		wisdom:GetMessageTemplate
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
SearchContent	Otorga permiso para buscar contenido que haga referencia a una base de conocimientos especificada. Se puede utilizar para obtener un recurso de contenido específico por su nombre	Lectura	KnowledgeBase*		
SearchMessageTemplates	Concede permiso para buscar plantillas de mensaje que hagan referencia a una base de conocimientos especificada	Lectura	KnowledgeBase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				wisdom:SearchFilter/RoutingProfileArn wisdom:SearchFilter/Qualifier	
SearchQuickResponses	Otorga permiso para buscar una respuesta rápida que haga referencia a una base de conocimientos especificada.	Lectura	KnowledgeBase*		wisdom:GetQuickResponse
				wisdom:SearchFilter/RoutingProfileArn	
SearchSessions	Otorga permiso para buscar sesiones que hacen referencia a un asistente especificado. Se puede utilizar para obtener un recurso de sesión específico por su nombre	Lectura			
SendMessage	Otorga permiso para enviar un mensaje	Escritura	Assistant*		
			Session*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartContentUpload	Otorga permiso para obtener una dirección URL para cargar contenido en una base de conocimientos	Escritura	KnowledgeBase*		
StartImportJob	Concede permiso para crear varias respuestas rápidas	Escritura	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Otorga permiso para agregar las etiquetas especificadas al recurso especificado	Etiquetado	Assistant		
			AssistantAssociation		
			Content		
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			Session		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para quitar las etiquetas especificadas de los recursos especificados	Etiquetado	Assistant		
			Assistant Association		
			Content		
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAIAgent	Concede permiso para actualizar la información sobre un agente de IA	Escritura	AIAgent*		
			Assistant*		
UpdateAIGuardrail	Otorga permiso para actualizar la información sobre una barandilla de aire	Escritura	AIGuardrail*		
			Assistant*		
UpdateAIPrompt	Concede permiso para actualizar la información sobre una petición de IA	Escritura	AIPrompt*		
			Assistant*		
UpdateAssistantAIAgent	Concede permiso para actualizar la información del asistente sobre un agente de IA	Escritura	Assistant*		
UpdateContent	Otorga permiso para actualizar la información sobre el contenido	Escritura	Content*		
			KnowledgeBase*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateKnowledgeBaseTemplateUri	Otorga permiso para actualizar la plantilla URI de una base de conocimientos	Escritura	KnowledgeBase*		
UpdateMessageTemplate	Concede permiso para actualizar el contenido de la plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
UpdateMessageTemplateMetadata	Concede permiso para actualizar los metadatos de la plantilla de mensaje	Escritura	KnowledgeBase*		
			MessageTemplate*		
UpdateQuickResponse	Otorga permiso para actualizar la información o el contenido de una respuesta rápida	Escritura	KnowledgeBase*		
			QuickResponse*		
UpdateSession	Concede permiso para actualizar una sesión	Escritura	Assistant*		
			Session*		
UpdateSessionData	Concede permiso para actualizar datos almacenados en una sesión	Escritura	Assistant*		
			Session*		

Tipos de recurso definidos por Amazon Q in Connect

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AIAgent	`arn:${Partition}:wisdom:${Region}:${Account}:ai-agent/${AssistantId}/${AIAgentId}`	aws:ResourceTag/${TagKey}
AIPrompt	`arn:${Partition}:wisdom:${Region}:${Account}:ai-prompt/${AssistantId}/${AIPromptId}`	aws:ResourceTag/${TagKey}
AIGuardrail	`arn:${Partition}:wisdom:${Region}:${Account}:ai-guardrail/${AssistantId}/${AIGuardrailId}`	aws:ResourceTag/${TagKey}
Assistant	`arn:${Partition}:wisdom:${Region}:${Account}:assistant/${AssistantId}`	aws:ResourceTag/${TagKey}
Assistant Association	`arn:${Partition}:wisdom:${Region}:${Account}:association/${AssistantId}/${AssistantAssociationId}`	aws:ResourceTag/${TagKey}
Content	`arn:${Partition}:wisdom:${Region}:${Account}:content/${KnowledgeBaseId}/${ContentId}`	aws:ResourceTag/${TagKey}
ContentAssociation	`arn:${Partition}:wisdom:${Region}:${Account}:content-association/${Knowl`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
	edgeBaseId}/${ContentId}/${ContentAssociationId}	
Knowledge Base	arn:${Partition}:wisdom:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
MessageTemplate	arn:${Partition}:wisdom:${Region}:${Account}:message-template/${KnowledgeBaseId}/${MessageTemplateId}	aws:ResourceTag/${TagKey} wisdom:MessageTemplate/RoutingProfileArn
Session	arn:${Partition}:wisdom:${Region}:${Account}:session/${AssistantId}/${SessionId}	aws:ResourceTag/${TagKey}
QuickResponse	arn:${Partition}:wisdom:${Region}:${Account}:quick-response/${KnowledgeBaseId}/${QuickResponseId}	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Q in Connect

Amazon Q in Connect define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
wisdom:MessageTemplate/RoutingProfileArn	Filtra el acceso por los ARN de perfil de enrutamiento de conexión asociados al recurso	ArrayOfARN
wisdom:SearchFilter/Qualifier	Filtra el acceso por los calificadores que se transmiten en la solicitud	ArrayOfString
wisdom:SearchFilter/RoutingProfileArn	Filtra el acceso según el perfil de enrutamiento de conexión (arn) que se incluye en la solicitud	ARN

Acciones, recursos y claves de condición para Amazon QLDB

Amazon QLDB(prefijo de servicio: `qldb`) proporciona las siguientes claves de contexto de condición, recursos y acciones específicas de servicios para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon QLDB
- Tipos de recurso definidos por Amazon QLDB
- Claves de condición de Amazon QLDB

Acciones definidas por Amazon QLDB

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelJournalKinesisStream	Otorga permiso para cancelar un flujo de Kinesis de diario	Write	stream*		
CreateLedger	Otorga permiso para crear un libro de contabilidad.	Write	ledger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLedger	Otorga permiso para eliminar un libro de contabilidad.	Write	ledger*		
DescribeJournalKinesisStream	Otorga permiso para describir información acerca de un flujo de Kinesis de diario	Read	stream*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeJournalS3Export	Otorga permiso para describir información acerca de un trabajo de exportación de diario.	Read	ledger*		
DescribeLedger	Otorga permiso para describir un libro de contabilidad	Lectura	ledger*		
ExecuteStatement [solo permiso]	Otorga permiso para enviar comandos a un libro de contabilidad a través de la consola.	Write	ledger*		
ExportJournalToS3	Otorga permiso para exportar el contenido del diario a un bucket de Amazon S3.	Escritura	ledger*		
GetBlock	Otorga permiso para recuperar un bloque de un libro mayor para un determinado BlockAddress	Lectura	ledger*		
GetDigest	Otorga permiso para recuperar un compendio de un libro mayor de un dato BlockAddress	Lectura	ledger*		
GetRevision	Otorga permiso para recuperar una revisión de un identificador de documento determinado y de un documento determinado BlockAddress	Lectura	ledger*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InsertSampleData [solo permiso]	Otorga permiso para insertar datos de aplicación de ejemplo a través de la consola.	Write	ledger*		
ListJournalKinesisStreamsForLedger	Otorga permiso para enumerar flujos de Kinesis de diario para un libro mayor específico	List	stream*		
ListJournalS3Exports	Otorga permiso para enumerar los trabajos de exportación de diario de todos los libros de contabilidad.	List			
ListJournalS3ExportsForLedger	Otorga permiso para enumerar los trabajos de exportación de diario de un libro de contabilidad mayor especificado.	List	ledger*		
ListLedgers	Otorga permiso para enumerar los libros de contabilidad existentes.	List			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Read	catalog		
			ledger		
			stream		
			table		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PartiQLCreateIndex	Otorga permiso para crear un índice en una tabla	Write	table*		
PartiQLCreateTable	Concede permiso para crear una tabla	Write	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PartiQLDelete	Otorga permiso para eliminar documentos de una tabla	Write	table*		
PartiQLDropIndex	Otorga permiso para eliminar un índice de una tabla	Write	table*		
				qldb:Purge	
PartiQLDropTable	Otorga permiso para colocar una tabla	Write	table*		
				qldb:Purge	
PartiQLHistoryFunction	Otorga permiso para utilizar la función de historial en una tabla	Read	table*		
PartiQLInsert	Otorga permiso para insertar documentos en una tabla	Escritura	table*		
PartiQLRedact	Concede permiso para redactar revisiones históricas	Escritura	table*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PartiQLSelect	Otorga permiso para seleccionar documentos de una tabla	Read	catalog		
			table		
PartiQLUndropTable	Otorga permiso para quitar una tabla	Write	table*		
PartiQLUpdate	Otorga permiso para actualizar documentos existentes en una tabla	Write	table*		
SendCommand	Otorga permiso para enviar comandos a un libro de contabilidad.	Escritura	ledger*		
ShowCatalog [solo permiso]	Otorga permiso para ver el catálogo de un libro de contabilidad a través de la consola.	Write	ledger*		
StreamJournalToKinesis	Otorga permiso para transmitir contenido de diario a un flujo de datos de Kinesis	Write	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso.	Etiquetado	catalog		
			ledger		
			stream		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	catalog		
			ledger		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateLedger	Otorga permiso para actualizar las propiedades de un libro de contabilidad.	Write	ledger*		
UpdateLedgerPermissionsMode	Otorga permiso para actualizar el modo de permisos en un libro mayor	Write	ledger*		

Tipos de recurso definidos por Amazon QLDB

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
ledger	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:qldb:${Region}:${Account}:stream/${LedgerName}/${StreamId}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/table/${TableId}`	aws:ResourceTag/${TagKey}
catalog	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/information_schema/user_tables`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon QLDB

Amazon QLDB define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
qldb:Purge	Filtra el acceso por el valor de purga especificado en una instrucción PartiQL DROP	Cadena

Acciones, recursos y claves de condición de Amazon QuickSight

Amazon QuickSight (prefijo de servicio:`quicksight`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon QuickSight
- Tipos de recursos definidos por Amazon QuickSight
- Claves de estado de Amazon QuickSight

Acciones definidas por Amazon QuickSight

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AccountConfigurations [solo permiso]	Otorga permiso para habilitar la configuración del acceso predeterminado a los recursos AWS	Escritura			
BatchCreateTopicReviewedAnswer	Concede permiso para crear respuestas revisadas para un tema	Escritura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchDeleteTopicReviewedAnswer	Concede permiso para eliminar respuestas revisadas para un tema	Escritura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelIngestion	Concede permiso para cancelar una incorporación de datos de SPICE en un conjunto de datos	Escritura	ingestion*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateAccountCustomization	Otorga permiso para crear una personalización de cuenta para la QuickSight cuenta o el espacio de nombres	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountSubscription	Otorga permiso para suscribirse a QuickSight	Escritura		quicksight:Edition quicksight:DirectoryType	
CreateAdmin [solo permiso]	Otorga permiso para aprovisionar a QuickSight los administradores, autores y lectores de Amazon	Escritura	user*		
CreateAnalysis	Concede permiso para crear un análisis a partir de una plantilla	Escritura	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrand	Otorga permiso para crear una QuickSight marca Amazon	Escritura	brand*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomPermissions	Otorga permiso para crear un recurso de permisos QuickSight personalizado	Escritura	custompermissions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Otorga permiso para crear un QuickSight panel	Escritura	dashboard*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Concede permiso para crear un conjunto de datos	Write	datasource*		quicksight:PassDataSource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Concede permiso para crear un origen de datos	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateEmailCustomizationTemplate [solo permiso]	Otorga permiso para crear una plantilla de personalización de QuickSight correo electrónico	Escritura	emailCustomizationTemplate*		
CreateFolder	Otorga permiso para crear una QuickSight carpeta	Escritura	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	Otorga permiso para añadir un QuickSight panel, un análisis o un conjunto de datos a una QuickSight carpeta	Escritura	folder*		
			analysis		
			dashboard		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			dataset		
CreateGroup	Otorga permiso para crear un QuickSight grupo	Escritura	group*		
CreateGroupMembership	Otorga permiso para añadir un QuickSight usuario a un QuickSight grupo	Escritura	group*	quicksight:UserName	
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIAMPolicyAssignment	Concede permiso para crear una asignación con un ARN de política de IAM específico que se asignará a grupos o usuarios específicos de QuickSight	Escritura	assignment*		
CreateIngestion	Concede permiso para iniciar una incorporación de datos de SPICE en un conjunto de datos	Escritura	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNamespace	Otorga permiso para crear un espacio de nombres QuickSight	Escritura	namespace*		ds:CreateIdentityPoolDirectory
CreateReader [solo permiso]	Concede permiso para aprovisionar QuickSight lectores de Amazon	Escritura	user*		
CreateRefreshSchedule	Concede permiso para crear un programa de actualización de un conjunto de datos	Escritura	refreshschedule*		
CreateRoleMembership	Concede permiso para agregar un miembro del grupo a un rol	Escritura		quicksight:Group identitystore:GroupId	
CreateTemplate	Concede permiso para crear una plantilla	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	Concede permiso para crear un alias de plantilla	Escritura	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTheme	Concede permiso para crear un tema.	Escritura	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	Concede permiso para crear un alias para una versión de tema	Escritura	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	Concede permiso para crear un tema	Escritura	dataset*		quicksight:PassDataSet

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	Concede permiso para crear un programa de actualización de un tema	Escritura	topic*		
CreateUser [solo permiso]	Otorga permiso para aprovisionar a QuickSight los autores y lectores de Amazon	Escritura	user*		
CreateVPCConnection	Concede permiso para crear una conexión de VPC	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomization	Otorga permiso para eliminar la personalización de una QuickSight cuenta o un espacio de nombres	Escritura	customization*		
DeleteAccountSubscription	Otorga permiso para eliminar una cuenta QuickSight	Escritura	account*		
DeleteAnalysis	Concede permiso para eliminar un análisis.	Escritura	analysis*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBrand	Otorga permiso para eliminar una QuickSight marca de Amazon	Escritura	brand*		
DeleteBrandAssignment	Otorga permiso para eliminar una asignación de marca	Escritura			
DeleteCustomPermissions	Otorga permiso para eliminar un recurso de permisos QuickSight personalizado	Escritura			
DeleteDashboard	Otorga permiso para eliminar un QuickSight panel	Escritura	dashboard*		
DeleteDataSet	Concede permiso para eliminar un conjunto de datos	Escritura	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	Concede permiso para eliminar las propiedades de actualización de un conjunto de datos	Escritura	dataset*		
DeleteDataSource	Concede permiso para eliminar un origen de datos	Escritura	datasource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDefaultQBusinessApplication	Otorga permiso para eliminar QBusiness la aplicación vinculada de la QuickSight cuenta	Escritura			
DeleteEmailCustomizationTemplate [solo permiso]	Otorga permiso para eliminar una plantilla de personalización de QuickSight correo electrónico	Escritura	emailCustomizationTemplate*		
DeleteFolder	Otorga permiso para eliminar una QuickSight carpeta	Escritura	folder*		
DeleteFolderMembership	Otorga permiso para eliminar un QuickSight panel, un análisis o un conjunto de datos de una QuickSight carpeta	Escritura	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	Otorga permiso para eliminar un grupo de usuarios de QuickSight	Escritura	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteGroupMembership	Otorga permiso para eliminar a un usuario de un grupo para que he/she deje de ser miembro del grupo	Escritura	group*	quicksight:UserName	
DeleteIAMPolicyAssignment	Concede permiso para actualizar una asignación existente	Escritura	assignment*		
DeleteIdentityPropagationConfig	Otorga permiso para eliminar AWS servicios de propagación de identidades confiables en QuickSight	Escritura			
DeleteNamespace	Otorga permiso para eliminar un QuickSight espacio de nombres	Escritura	namespace*		ds:DeleteDirectory
DeleteRefreshSchedule	Concede permiso para eliminar un programa de actualización de un conjunto de datos	Escritura	refreshschedule*		
DeleteRoleCustomPermission	Concede permiso para eliminar el permiso personalizado asociado a un rol	Escritura			
DeleteRoleMembership	Concede permiso para eliminar a un miembro del grupo de un rol	Escritura		quicksight:Group identitystore:GroupId	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTemplate	Concede permiso para eliminar una plantilla	Write	template*		
DeleteTemplateAlias	Concede permiso para eliminar un alias de plantilla	Write	template*		
DeleteTheme	Concede permiso para eliminar un tema	Write	theme*		
DeleteThemeAlias	Concede permiso para eliminar el alias de un tema	Escritura	theme*		
DeleteTopic	Concede permiso para eliminar un tema	Escritura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTopicRefreshSchedule	Concede permiso para eliminar un programa de actualización de un tema	Escritura	topic*		
DeleteUser	Otorga permiso para eliminar un QuickSight usuario, dado el nombre de usuario	Escritura	user*		
DeleteUserByPrincipalId	Concede permiso para eliminar a un usuario identificado por su ID principal	Escritura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUserCustomPermission	Otorga permiso para eliminar el permiso personalizado asociado a un usuario	Escritura	user*		
DeleteVPCConnection	Concede permiso para eliminar una conexión de VPC	Escritura	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAccountCustomization	Otorga permiso para describir la personalización de una cuenta para una QuickSight cuenta o un espacio de nombres	Lectura	customization*		
DescribeAccountSettings	Otorga permiso para describir la configuración administrativa de la cuenta QuickSight	Lectura			
DescribeAccountSubscription	Otorga permiso para describir una QuickSight cuenta	Lectura	account*		
DescribeAnalysis	Concede permiso para describir un análisis	Read	analysis*		
DescribeAnalysisPermissions	Concede permiso para describir los permisos de un análisis	Lectura	analysis*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAssetBundleExportJob	Concede permiso para describir un trabajo de exportación de paquetes de activos	Lectura	assetBundleExportJob*		
DescribeAssetBundleImportJob	Concede permiso para describir un trabajo de importación de paquetes de activos	Lectura	assetBundleImportJob*		
DescribeBrand	Otorga permiso para describir una marca	Lectura	brand*		
DescribeBrandAssignment	Otorga permiso para describir una asignación de marca	Lectura			
DescribeBrandPublishedVersion	Otorga permiso para describir la versión publicada de la marca	Lectura	brand*		
DescribeCustomPermissions	Otorga permiso para describir un recurso de permisos personalizados en una QuickSight cuenta	Lectura	custompermissions*		
DescribeDashboard	Otorga permiso para describir un QuickSight panel	Lectura	dashboard*		
DescribeDashboardPermissions	Otorga permiso para describir los permisos de un QuickSight panel	Lectura	dashboard*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDashboardSnapshotJob	Otorga permiso para describir un trabajo de instantánea del tablero	Lectura	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	Otorga permiso para describir el resultado de un trabajo de instantánea del tablero	Lectura	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	Otorga permiso para describir una configuración de los paneles	Lectura			
DescribeDataSet	Concede permiso para describir un conjunto de datos	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetPermissions	Concede permiso para describir la política de recursos de un conjunto de datos	Administración de permisos	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDataSetRefreshProperties	Concede permiso para describir las propiedades de actualización de un conjunto de datos	Lectura	dataset*		
DescribeDataSource	Concede permiso para describir un origen de datos	Read	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSourcePermissions	Concede permiso para describir la política de recursos de un origen de datos	Administración de permisos	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDefaultQBusinessApplication	Otorga permiso para describir el identificador de QBusiness la aplicación vinculada a la cuenta QuickSight	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEmailCustomizationTemplate [solo permiso]	Otorga permiso para describir una plantilla de personalización de QuickSight correo electrónico	Lectura	emailCustomizationTemplate*		
DescribeFolder	Otorga permiso para describir una QuickSight carpeta	Lectura	folder*		
DescribeFolderPermissions	Otorga permiso para describir los permisos de una QuickSight carpeta	Lectura	folder*		
DescribeFolderResolvedPermissions	Otorga permiso para describir los permisos resueltos para una QuickSight carpeta	Lectura	folder*		
DescribeGroup	Otorga permiso para describir un QuickSight grupo	Lectura	group*		
DescribeGroupMembership	Otorga permiso para describir a un miembro QuickSight del grupo	Lectura	group*	quicksight:UserName	
DescribeIAMPolicyAssignment	Concede permiso para describir una asignación existente	Read	assignment*		
DescribeIngestion	Concede permiso para describir una incorporación de datos de SPICE a un conjunto de datos	Lectura	ingestion*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	Otorga permiso para describir las restricciones de IP de la QuickSight cuenta	Lectura			
DescribeKeyRegistration	Otorga permiso para describir el registro de QuickSight claves	Lectura			
DescribeNamespace	Otorga permiso para describir un QuickSight espacio de nombres	Lectura	namespace*		
DescribeQPersonalizationConfiguration	Concede permiso para describir una configuración de personalización	Lectura			
DescribeQuickSightQSearchConfiguration	Otorga permiso para describir la configuración de QuickSight Q Search	Lectura			
DescribeRefreshSchedule	Concede permiso para describir un programa de actualización de un conjunto de datos	Lectura	refreshschedule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRoleCustomPermission	Concede permiso para describir el permiso personalizado asociado a un rol	Lectura			
DescribeTemplate	Concede permiso para describir una plantilla	Read	template*		
DescribeTemplateAlias	Concede permiso para describir un alias de plantilla	Read	template*		
DescribeTemplatePermissions	Concede permiso para describir los permisos de una plantilla	Read	template*		
DescribeTheme	Concede permiso para describir un tema	Read	theme*		
DescribeThemeAlias	Concede permiso para describir un alias de tema	Read	theme*		
DescribeThemePermissions	Concede permiso para describir los permisos de un tema	Lectura	theme*		
DescribeTopic	Concede permiso para describir un tema	Lectura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeTopicPermissions	Concede permiso para describir la política de recursos de un tema	Administración de permisos	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	Concede permiso para describir el estado de actualización de un tema	Lectura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefreshSchedule	Concede permiso para describir un programa de actualización de un tema	Lectura	topic*		
DescribeUser	Otorga permiso para describir a un QuickSight usuario dado el nombre de usuario	Lectura	user*		
DescribeVPCConnection	Concede permiso para describir una conexión de VPC	Lectura	vpcconnection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
GenerateEmbedUrlForAnonymousUser	Otorga permiso para generar una URL que se utilice para incrustar un QuickSight panel de control o un tema para un usuario no registrado QuickSight	Escritura	namespace*		
			dashboard		
			theme		
			topic		
				aws:TagKeys aws:RequestTag/${TagKey} quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUser	Otorga permiso para generar una URL utilizada para incrustar un QuickSight panel de control para un usuario registrado en QuickSight	Escritura	user*		
				quicksight:AllowedEmbeddingDomains	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateEmbedUrlForRegisteredUserWithIdentity	Otorga permiso para generar una URL que se utilice para integrar una QuickSight experiencia a un usuario registrado QuickSight con una sesión de rol mejorada	Escritura		quicksight:AllowedEmbeddingDomains	
GetAnonymousUserEmbedUrl [solo permiso]	Otorga permiso para que un usuario no registrado pueda utilizar una URL para incrustar un QuickSight panel QuickSight	Lectura			
GetAuthCode [solo permiso]	Otorga permiso para obtener un código de autenticación que represente a un usuario QuickSight	Lectura	user*		
GetDashboardEmbedUrl	Otorga permiso para utilizar una URL para incrustar un panel QuickSight	Lectura	dashboard*		
GetGroupMapping [solo permiso]	Otorga permiso para usar Amazon QuickSight, en la edición Enterprise, para identificar y mostrar los grupos de directorios de Microsoft Active Directory (Microsoft Active Directory) que están asignados a funciones en Amazon QuickSight	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSessionEmbedUrl	Otorga permiso para obtener una URL para integrar la experiencia de QuickSight la consola	Lectura			
ListAnalyses	Concede permiso para enumerar todos los análisis de una cuenta	Enumeración	analysis*		
ListAssetBundleExportJobs	Concede permiso para enumerar todos los trabajos de exportación de paquetes de activos	Enumeración	assetBundleExportJob*		
ListAssetBundleImportJobs	Concede permiso para enumerar todos los trabajos de importación de paquetes de activos	Enumeración	assetBundleImportJob*		
ListBrands	Otorga permiso para publicar todas las marcas en una QuickSight cuenta de Amazon	Enumeración			
ListCustomPermissions	Otorga permiso para incluir permisos personalizados y recursos en la QuickSight cuenta	Enumeración			
ListCustomerManagedKeys [solo permiso]	Concede permiso para enumerar todas las claves administradas por los clientes registradas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDashboardVersions	Otorga permiso para enumerar todas las versiones de un QuickSight panel	Enumeración	dashboard*		
ListDashboards	Otorga permiso para enumerar todos los paneles de una cuenta QuickSight	Enumeración	dashboard*		
ListDataSets	Concede permiso para enumerar todos los conjuntos de datos	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	Concede permiso para enumerar todos los orígenes de datos	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListFolderMembers	Concede permiso para enumerar todos los miembros de una carpeta	Lectura	folder*		
ListFolders	Otorga permiso para enumerar todas las carpetas de una cuenta QuickSight	Enumeración	folder*		
ListFoldersForResource	Otorga permiso para enumerar todas las carpetas de las que forma parte un QuickSight recurso	Enumeración	analysis dashboard		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			dataset		
			datasource		
			topic		
ListGroupMemberships	Concede permiso para enumerar a los usuarios miembros de un grupo	Enumeración	group*		
ListGroups	Otorga permiso para enumerar todos los grupos de usuarios de QuickSight	Enumeración	group*		
ListIAMPolicyAssignments	Otorga permiso para publicar todas las tareas de la QuickSight cuenta Amazon actual	Enumeración	assignment*		
ListIAMPolicyAssignmentsForUser	Concede permiso para enumerar todas las asignaciones realizadas a un usuario y a los grupos a los que pertenece	Enumeración	assignment*		
ListIdentityPropagationConfigs	Otorga permiso para enumerar AWS los servicios habilitados para la propagación de identidades confiables en QuickSight	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIngestions	Concede permiso para enumerar todas las incorporaciones de datos de SPICE a un conjunto de datos	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser [solo permiso]	Concede permiso para enumerar las claves KMS de un usuario	Enumeración			
ListNamespaces	Otorga permiso para enumerar todos los espacios de nombres de una cuenta QuickSight	Enumeración			
ListRefreshSchedules	Concede permiso para enumerar todos los programas de actualización de un conjunto de datos	Enumeración			
ListRoleMemberships	Concede permiso para enumerar a los miembros de un rol	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso QuickSight	Lectura	analysis		
			brand		
			customization		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			template		
			theme		
			topic		
			vpcconnection		
ListTemplateAliases	Concede permiso para enumerar todos los alias de una plantilla	List	template*		
ListTemplateVersions	Concede permiso para enumerar todas las versiones de una plantilla	Enumeración	template*		
ListTemplates	Otorga permiso para enumerar todas las plantillas de una QuickSight cuenta	Enumeración	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListThemeAliases	Concede permiso para enumerar todos los alias de un tema	List	theme*		
ListThemeVersions	Concede permiso para enumerar todas las versiones de un tema	List	theme*		
ListThemes	Concede permiso para enumerar todos los temas de una cuenta	Enumeración	theme*		
ListTopicRefreshSchedules	Concede permiso para enumerar todos los programas de actualización de un tema	Enumeración			
ListTopicReviewedAnswers	Concede permiso para enumerar todas las respuestas revisadas para el tema	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListTopics	Concede permiso para enumerar todos los temas	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
ListUserGroups	Concede permiso para enumerar los grupos de los cuales un usuario determinado es miembro	Enumeración	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListUsers	Otorga permiso para enumerar todos los QuickSight usuarios que pertenecen a esta cuenta	Enumeración	user*		
ListVPCConnections	Concede permiso para enumerar todas las conexiones de VPC	Enumeración		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet [solo permiso]	Concede permiso para usar un conjunto de datos para una plantilla	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSource [solo permiso]	Concede permiso para utilizar un origen de datos para un conjunto de datos	Lectura	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PredictQAResults	Otorga permiso para predecir los resultados del control de calidad	Lectura	dashboard		
			topic		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutDataSetRefreshProperties	Concede permiso para colocar las propiedades de actualización de un conjunto de datos	Escritura	dataset*		
RegisterCustomerManagedKey [solo permiso]	Concede permiso para registrar una clave administrada por un cliente	Escritura			
RegisterUser	Otorga permiso para crear un QuickSight usuario cuya identidad esté asociada al IAM identity/role especificado en la solicitud	Escritura	user*	quicksight:IamArn quicksight:SessionName	
RemoveCustomerManagedKey [solo permiso]	Concede permiso para eliminar una clave administrada por un cliente	Escritura			
RestoreAnalysis	Concede permiso para restaurar un análisis eliminado	Escritura	analysis*		
ScopeDownPolicy [solo permiso]	Otorga permiso para administrar las políticas de alcance de los permisos a los recursos AWS	Escritura			
SearchAnalyses	Concede permiso para buscar un subconjunto de análisis	Enumeración	analysis*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchDashboards	Otorga permiso para buscar un subconjunto de paneles QuickSight	Enumeración	dashboard*		
SearchDataSets	Otorga permiso para buscar un subconjunto de QuickSight DatSets	Enumeración	dataset*		
SearchDataSources	Otorga permiso para buscar un subconjunto de fuentes de datos QuickSight	Enumeración	datasource*		
SearchDirectoryGroups [solo permiso]	Otorga permiso para usar Amazon QuickSight, en la edición Enterprise, para mostrar sus grupos de directorios de Microsoft Active Directory para que pueda elegir cuáles asignar a las funciones en Amazon QuickSight	Enumeración			
SearchFolders	Otorga permiso para buscar un subconjunto de carpetas QuickSight	Lectura	folder*		
SearchGroups	Otorga permiso para buscar un subconjunto de grupos QuickSight	Enumeración	group*		
SearchTopics	Otorga permiso para buscar un subconjunto de temas	Enumeración	topic*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchUsers [solo permiso]	Otorga permiso para buscar a los QuickSight usuarios que pertenecen a esta cuenta	Enumeración	user*		
SetGroupMapping [solo permiso]	Otorga permiso para usar Amazon QuickSight, en la edición Enterprise, para mostrar sus grupos de directorios de Microsoft Active Directory para que pueda elegir cuáles asignar a las funciones en Amazon QuickSight	Escritura			
StartAssetBundleExportJob	Concede permiso para iniciar un trabajo de exportación de paquetes de activos	Escritura	assetBundleExportJob*		
StartAssetBundleImportJob	Concede permiso para iniciar un trabajo de importación de paquetes de activos	Escritura	assetBundleImportJob*		
StartDashboardSnapshotJob	Otorga permiso para iniciar un trabajo de instantánea del tablero	Escritura	dashboardSnapshotJob*		
StartDashboardSnapshotJobSchedule	Concede permiso para iniciar una programación de trabajo de instantánea de panel	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Subscribe [solo permiso]	Otorga permiso para suscribirse a Amazon QuickSight y también para permitir al usuario actualizar la suscripción a la edición Enterprise	Escritura		quicksight:Edition quicksight:DirectoryType	
TagResource	Otorga permiso para añadir etiquetas a un QuickSight recurso	Etiquetado	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
Unsubscribe [solo permiso]	Otorga permiso para cancelar la suscripción a Amazon QuickSight, lo que elimina permanentemente a todos los usuarios y sus recursos de Amazon QuickSight	Escritura			
UntagResource	Otorga permiso para eliminar etiquetas de un recurso QuickSight	Etiquetado	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys	
UpdateAccountCustomization	Otorga permiso para actualizar la personalización de una QuickSight cuenta o un espacio de nombres	Escritura	customization*		
UpdateAccountSettings	Otorga permiso para actualizar la configuración administrativa de la cuenta QuickSight	Escritura			
UpdateAnalysis	Concede permiso para actualizar un análisis	Write	analysis*		
UpdateAnalysisPermissions	Concede permiso para actualizar los permisos de un análisis	Administración de permisos	analysis*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApplicationWithTokenExchangeGrant	Otorga permiso para actualizar la aplicación QuickSight IAM Identity Center con el permiso de Token Exchange	Escritura			
UpdateBrand	Otorga permiso para actualizar una marca	Escritura	brand*		
UpdateBrandAssignment	Otorga permiso para actualizar una asignación de marca	Escritura			
UpdateBrandPublishedVersion	Otorga permiso para actualizar la versión publicada de una marca	Escritura	brand*		
UpdateCustomPermissions	Otorga permiso para actualizar un recurso de permisos QuickSight personalizado	Escritura	custompermissions*		
UpdateDashboard	Otorga permiso para actualizar un QuickSight panel	Escritura	dashboard*		
UpdateDashboardLinks	Otorga permiso para actualizar los enlaces de un QuickSight panel	Escritura	dashboard*		
UpdateDashboardPermissions	Otorga permiso para actualizar los permisos de un QuickSight panel	Administración de permisos	dashboard*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDashboardPublishedVersion	Otorga permiso para actualizar la versión publicada de un QuickSight panel	Escritura	dashboard*		
UpdateDashboardsQAConfiguration	Otorga permiso para actualizar la configuración de los paneles	Escritura			
UpdateDataSet	Concede permiso para actualizar un conjunto de datos	Write	dataset*		quicksight:PassDataSource
			datasource		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSetPermissions	Concede permiso para actualizar la política de recursos de un conjunto de datos	Permissions management	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	Concede permiso para actualizar un origen de datos	Write	datasource*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSourcePermissions	Concede permiso para actualizar la política de recursos de un origen de datos	Administración de permisos	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDefaultQBusinessApplication	Otorga permiso para actualizar el identificador de QBusiness la aplicación vinculada a la cuenta QuickSight	Escritura			
UpdateEmailCustomizationTemplate [solo permiso]	Otorga permiso para actualizar una plantilla de personalización de QuickSight correo electrónico	Escritura	emailCustomizationTemplate*		
UpdateFolder	Otorga permiso para actualizar una QuickSight carpeta	Escritura	folder*		
UpdateFolderPermissions	Otorga permiso para actualizar los permisos de una QuickSight carpeta	Administración de permisos	folder*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGroup	Concede permiso para cambiar la descripción del grupo	Write	group*		
UpdateIAMPolicyAssignment	Concede permiso para actualizar una asignación existente	Escritura	assignment*		
UpdateIdentityPropagationConfig	Otorga permiso para añadir y actualizar AWS servicios para la propagación de identidades confiables en QuickSight	Escritura			
UpdateIpRestriction	Otorga permiso para actualizar las restricciones de IP de la QuickSight cuenta	Escritura			
UpdateKeyRegistration	Otorga permiso para actualizar el registro de QuickSight claves	Escritura			
UpdatePublicSharingSettings	Concede permiso para habilitar o deshabilitar el uso compartido público en una cuenta	Escritura			
UpdateQPersonalizationConfiguration	Concede permiso para actualizar una configuración de personalización	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateQuickSightQSearchConfiguration	Otorga permiso para actualizar la configuración de QuickSight Q Search	Escritura			
UpdateRefreshSchedule	Concede permiso para actualizar un programa de actualización de un conjunto de datos	Escritura	refreshschedule*		
UpdateResourcePermissions [solo permiso]	Otorga permiso para actualizar los permisos a nivel de recurso en QuickSight	Escritura			
UpdateRoleCustomPermission	Concede permiso para actualizar el permiso personalizado asociado a un rol	Escritura			
UpdateSPICECapacityConfiguration	Otorga permiso para actualizar la configuración de capacidad de QuickSight SPICE	Escritura			
UpdateTemplate	Concede permiso para actualizar una plantilla	Write	template*		
UpdateTemplateAlias	Concede permiso para actualizar el alias de una plantilla	Write	template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTemplatePermissions	Concede permiso para actualizar los permisos de una plantilla	Permissions management	template*		
UpdateTheme	Concede permiso para actualizar un tema	Write	theme*		
UpdateThemeAlias	Concede permiso para actualizar el alias de un tema	Write	theme*		
UpdateThemePermissions	Concede permiso para actualizar los permisos de un tema	Administración de permisos	theme*		
UpdateTopic	Concede permiso para actualizar un tema	Escritura	topic*		quicksight:PassDataSet
			dataset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	Concede permiso para actualizar la política de recursos de un tema	Administración de permisos	topic*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicRefreshSchedule	Concede permiso para actualizar un programa de actualización de un tema	Escritura	topic*		
UpdateUser	Otorga permiso para actualizar un QuickSight usuario de Amazon	Escritura	user*		
UpdateUserCustomPermission	Otorga permiso para actualizar el permiso personalizado asociado a un usuario	Escritura	user*		
UpdateVPCConnection	Concede permiso para actualizar una conexión de VPC	Escritura	vpcconnection*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos por Amazon QuickSight

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
account	`arn:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}`	
user	`arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}`	
group	`arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}`	
analysis	`arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey}
vpcconnection	`arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}`	aws:ResourceTag/${TagKey}
assetBundleExportJob	`arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}`	
assetBundleImportJob	`arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}`	

Tipos de recurso	ARN	Claves de condición
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	

Tipos de recurso	ARN	Claves de condición
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard SnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}
brand	arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}	aws:ResourceTag/${TagKey}
custompermissions	arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}	aws:ResourceTag/${TagKey}

Claves de estado de Amazon QuickSight

Amazon QuickSight define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta	ArrayOfString

Claves de condición	Descripción	Tipo
identitystore:GroupId	Filtra el acceso por IdentityStore ARN de grupo	ARN
quicksight:AllowedEmbeddingDomains	Filtra el acceso según los dominios de integración permitidos.	ArrayOfString
quicksight:DirectoryType	Filtra el acceso mediante las opciones de administración de usuarios	Cadena
quicksight:Edition	Filtra el acceso por edición de QuickSight	Cadena
quicksight:Group	Filtra el acceso por QuickSight ARN de grupo	ARN
quicksight:IamArn	Filtra el acceso por el ARN del usuario o del rol de IAM	ARN
quicksight:KmsKeyArns	Filtra el acceso por clave KMS ARNs	ArrayOfARN
quicksight:SessionName	Filtra el acceso por el nombre de la sesión	Cadena
quicksight:UserName	Filtra el acceso por el nombre de usuario	Cadena

Acciones, recursos y claves de condición de la API de datos de Amazon RDS

La API de datos de Amazon RDS (prefijo de servicio: `rds-data`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la API de datos de Amazon RDS
- Tipos de recurso definidos por la API de datos de Amazon RDS
- Claves de condición de la API de datos de Amazon RDS

Acciones definidas por la API de datos de Amazon RDS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchExecuteStatement	Otorga permiso para ejecutar una instrucción SQL por lotes sobre una matriz de datos	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
BeginTransaction	Otorga permiso para iniciar una transacción SQL	Escritura	cluster*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CommitTransaction	Otorga permiso para finalizar una transacción de SQL iniciada con la BeginTransaction operación y confirma los cambios	Escritura	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteSql	Otorga permiso para ejecutar una o más instrucciones SQL Esta operación está obsoleta. Utilice la ExecuteStatement operación BatchExecuteStatement o	Escritura	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteStatement	Otorga permiso para ejecutar una instrucción SQL en una base de datos	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RollbackTransaction	Otorga permiso para llevar a cabo la restauración de una transacción. Si restaura una transacción, cancelará sus cambios.	Write	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recurso definidos por la API de datos de Amazon RDS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} aws:TagKeys

Claves de condición de la API de datos de Amazon RDS

La API de datos de Amazon RDS define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso según las claves de la etiqueta asociada con el recurso	ArrayOfString

Acciones, recursos y claves de condición para la autenticación IAM de Amazon RDS

La autenticación IAM de Amazon RDS (prefijo de servicio: `rds-db`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la autenticación IAM de Amazon RDS
- Tipos de recursos definidos por la autenticación de IAM de Amazon RDS
- Claves de condición para la autenticación IAM de Amazon RDS

Acciones definidas por la autenticación IAM de Amazon RDS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
connect	Permite que el rol o el usuario de IAM se conecte a la base de datos de RDS	Permissions management	db-user*		

Tipos de recursos definidos por la autenticación de IAM de Amazon RDS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Claves de condición para la autenticación IAM de Amazon RDS

La autenticación IAM de RDS no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para la papelera de reciclaje de AWS

AWS La papelera de reciclaje (prefijo de servicio:`rbin`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la papelera de reciclaje de AWS
- Tipos de recurso definidos por la papelera de reciclaje de AWS
- Claves de condición de la papelera de reciclaje de AWS

Acciones definidas por la papelera de reciclaje de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRule	Otorga permiso para crear una regla de retención de la papelera de reciclaje.	Escritura	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				rbin:Request/ResourceType	
DeleteRule	Otorga permiso para eliminar una regla de retención de la papelera de reciclaje.	Escritura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	Otorga permiso para obtener información detallada acerca de una regla de retención de la papelera de reciclaje.	Lectura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
ListRules	Otorga permiso para enumerar las reglas de retención de la papelera de reciclaje en la región.	Lectura		rbin:Request/ResourceType	
ListTagsForResource	Otorga permiso para enumerar las etiquetas asociadas a un recurso.	Lectura	rule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	Otorga permiso para bloquear una regla de retención existente de la papelera de reciclaje	Escritura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
TagResource	Otorga permiso para agregar o actualizar las etiquetas de un recurso.	Etiquetado	rule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UnlockRule	Otorga permiso para desbloquear una regla de retención existente de la papelera de reciclaje	Escritura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
UntagResource	Concede permiso para eliminar las etiquetas asociadas a un recurso	Etiquetado	rule*		
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	Otorga permiso para actualizar una regla de retención existente de la papelera de reciclaje.	Escritura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Tipos de recurso definidos por la papelera de reciclaje de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
rule	`arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}`	aws:ResourceTag/${TagKey}

Claves de condición de la papelera de reciclaje de AWS

AWS La papelera de reciclaje define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
rbin:Attribute/ResourceType	Filtra el acceso por el tipo del recurso de la regla existente	Cadena
rbin:Request/ResourceType	Filtra el acceso por el tipo del recurso en una solicitud	Cadena

Acciones, recursos y claves de condición para Amazon Redshift

Amazon Redshift (prefijo de servicio: `redshift`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Redshift
- Tipos de recursos definidos por Amazon Redshift
- Claves de condición de Amazon Redshift

Acciones definidas por Amazon Redshift

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptReservedNodeExchange	Otorga permiso para intercambiar un nodo DC1 reservado por un nodo DC2 reservado sin cambios en la configuración	Escritura			
AddPartner	Concede permiso para agregar una integración de socios a un clúster	Escritura			
AssociateDataShareConsumer	Concede permiso para asociar un consumidor a un recurso compartido de datos	Write	datashare*		
				redshift:ConsumerArn redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	Concede permiso para agregar una regla de entrada a un grupo de seguridad de Amazon Redshift	Escritura	securitygroup*		
			securitygroupingress-ec2securitygroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AuthorizeDataShare	Concede permiso para autorizar al consumidor del recurso compartido de datos especificado a consumir ese recurso compartido de datos	Administración de permisos	datashare*		
				redshift:ConsumerIdentifier redshift:AllowWrites	
AuthorizeEndpointAccess	Concede permiso para autorizar actividades relacionadas con puntos de conexión para un punto de conexión de VPC administrado por redshift	Administración de permisos			
AuthorizeInboundIntegration [solo permiso]	Concede permiso a Amazon Redshift para validar continuamente que el almacén de datos de destino pueda recibir los datos replicados desde el ARN de origen	Escritura	integration*		
AuthorizeSnapshotAccess	Otorga permiso al especificado Cuenta de AWS para restaurar una instantánea	Administración de permisos	snapshot*		
BatchDeleteClusterSnapshots	Concede permiso para eliminar instantáneas de un lote, hasta 100	Write	snapshot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchModifyClusterSnapshots	Concede permiso para modificar la configuración de una lista de instantáneas	Write	snapshot*		
CancelQuery [solo permiso]	Concede permiso para cancelar una consulta a través de la consola de Amazon Redshift	Write			
CancelQuerySession [solo permiso]	Concede permiso para ver consultas en la consola de Amazon Redshift	Write			
CancelResize	Concede permiso para cancelar una operación de cambio de tamaño	Write	cluster*		
CopyClusterSnapshot	Concede permiso para copiar una instantánea del clúster	Escritura	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAuthenticationProfile	Concede permiso para crear un perfil de autenticación de Amazon Redshift	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCluster	Concede permiso para crear un clúster	Write	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Concede permiso para crear un grupo de parámetros de Amazon Redshift	Write	parametergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSecurityGroup	Concede permiso para crear un grupo de seguridad de Amazon Redshift	Write	securitygroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	Concede permiso para crear una instantánea manual del clúster especificado	Write	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	Concede permiso para crear un grupo de subredes de Amazon Redshift	Write	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	Concede permiso para crear automáticamente el usuario de Amazon Redshift especificado si no existe	Administración de permisos	dbuser*		
				redshift:DbUser	
CreateCustomDomainAssociation	Otorga permiso para crear un nombre de dominio personalizado para un clúster	Escritura	cluster*		acm:DescribeCertificate

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEndpointAccess	Concede permiso para crear un punto de conexión de VPC administrado por redshift	Escritura			
CreateEventSubscription	Concede permiso para crear una suscripción de notificación de evento de Amazon Redshift	Write	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	Concede permiso para crear un certificado de cliente de HSM que un clúster utiliza para conectarse a un HSM	Write	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmConfiguration	Concede permiso para crear una configuración de HSM que contenga la información requerida por un clúster para almacenar y utilizar las claves de cifrado de base de datos en un módulo de seguridad de hardware (HSM)	Write	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInboundIntegration [solo permiso]	Concede permiso a la entidad principal de origen para crear una integración entrante de modo que los datos se repliquen desde el origen hacia el almacenamiento de datos de destino	Escritura			
CreateIntegration	Concede permiso para crear una integración sin ETL de Amazon Redshift	Escritura	integration*		kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys redshift:IntegrationSourceArn redshift:IntegrationTargetArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateQev2IdcApplication [solo permiso]	Concede permiso para crear una aplicación QEV2 IDC	Escritura			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRedshiftIdcApplication	Concede permiso para crear una aplicación redshift idc	Escritura			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery [solo permiso]	Concede permiso para crear consultas SQL guardadas a través de la consola de Amazon Redshift	Write			
CreateScheduledAction	Concede permiso para crear una acción programada de Amazon Redshift	Escritura			
CreateSnapshotCopyGrant	Otorga permiso para crear una copia instantánea, conceder y cifrar las instantáneas copiadas en un destino Región de AWS	Administración de permisos	snapshotcopygrant*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotSchedule	Concede permiso para crear una programación de instantáneas	Write	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Concede permiso para agregar una o varias etiquetas a un recurso especificado	Etiquetado	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateUsageLimit	Concede permiso para crear un límite de uso	Escritura	usagelimit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	Concede permiso para quitar permiso al consumidor del recurso compartido de datos especificado de modo que no consuma ese recurso compartido de datos	Administración de permisos	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	Concede permiso para eliminar un perfil de autenticación de Amazon Redshift	Escritura			
DeleteCluster	Concede permiso para eliminar un clúster aprovisionado anteriormente	Write	cluster*		
DeleteClusterParameterGroup	Concede permiso para eliminar un grupo de parámetros de Amazon Redshift	Write	parametergroup*		
DeleteClusterSecurityGroup	Concede permiso para eliminar un grupo de seguridad de Amazon Redshift	Write	securitygroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteClusterSnapshot	Concede permiso para eliminar una instantánea manual	Write	snapshot*		
DeleteClusterSubnetGroup	Concede permiso para eliminar un grupo de subredes del clúster	Escritura	subnetgroup*		
DeleteCustomDomainAssociation	Otorga permiso para eliminar un nombre de dominio personalizado para un clúster	Escritura	cluster*		
DeleteEndpointAccess	Concede permiso para eliminar un punto de conexión de VPC administrado por redshift	Escritura			
DeleteEventSubscription	Concede permiso para eliminar una suscripción de notificación de eventos de Amazon Redshift	Write	eventsubscription*		
DeleteHsmClientCertificate	Concede permiso para eliminar un certificado del cliente de HSM	Write	hsmclientcertificate*		
DeleteHsmConfiguration	Concede permiso para eliminar una configuración de HSM de Amazon Redshift	Escritura	hsmconfiguration*		
DeleteIntegration	Concede permiso para eliminar una integración sin ETL de Amazon Redshift	Escritura	integration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeletePartner	Concede permiso para eliminar una integración de socios de un clúster	Escritura			
DeleteQev2IdcApplication [solo permiso]	Concede permiso para eliminar una aplicación QEV2 IDC	Escritura	qev2idcapplication*		sso:DeleteApplication
DeleteRedshiftIdcApplication	Concede permiso para eliminar una aplicación redshift idc	Escritura	redshiftidcapplication*		sso:DeleteApplication
DeleteResourcePolicy	Concede permiso para eliminar la política de recursos para un recurso especificado	Administración de permisos	namespace*		
DeleteSavedQueries [solo permiso]	Concede permiso para eliminar consultas SQL guardadas a través de la consola de Amazon Redshift	Write			
DeleteScheduledAction	Concede permiso para eliminar una acción programada de Amazon Redshift	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSnapshotCopyGrant	Concede permiso para eliminar una concesión de copia de instantáneas	Write	snapshotcopygrant*		
DeleteSnapshotSchedule	Concede permiso para eliminar una programación de instantáneas	Write	snapshotschedule*		
DeleteTags	Concede permiso para eliminar una o varias etiquetas de un recurso	Etiquetado	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:TagKeys	
DeleteUsageLimit	Concede permiso para eliminar un límite de uso	Escritura	usagelimit*		
DeregisterNamespace	Otorga permiso a un consumidor para anular el registro del espacio de nombres especificado	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAccountAttributes	Otorga permiso para describir los atributos adjuntos al especificado Cuenta de AWS	Lectura			
DescribeAuthenticationProfiles	Concede permiso para describir los perfiles de autenticación de Amazon Redshift creados	Lectura			
DescribeClusterDbRevisions	Concede permiso para describir las revisiones de la base de datos de un clúster	List			
DescribeClusterParameterGroups	Concede permiso para describir los grupos de parámetros de Amazon Redshift, incluidos aquellos que usted ha creado y el grupo de parámetros predeterminado	Read			
DescribeClusterParameters	Concede permiso para describir los parámetros incluidos en un grupo de parámetros de Amazon Redshift	Read	parametergroup*		
DescribeClusterSecurityGroups	Concede permiso para describir los grupos de seguridad de Amazon Redshift	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeClusterSnapshots	Concede permiso para describir uno o varios objetos de instantánea, que contienen metadatos sobre las instantáneas del clúster	Read			
DescribeClusterSubnetGroups	Devuelve uno o varios objetos del grupo de subredes del clúster, que contienen los metadatos de los grupos de subredes del clúster.	Read			
DescribeClusterTracks	Concede permiso para describir los registros de seguimiento de mantenimiento disponibles	List			
DescribeClusterVersions	Concede permiso para describir las versiones disponibles del clúster de Amazon Redshift	Read			
DescribeClusters	Concede permiso para describir las propiedades de los clústeres aprovisionados	Enumeración			
DescribeCustomDomainAssociations	Otorga permiso para describir nombres de dominio personalizados para un clúster	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDataShares	Concede permiso para describir el recurso compartido de datos creado y consumido por los clústeres	Read			
DescribeDataSharesForConsumer	Concede permiso para describir solo el recurso compartido de datos consumido por los clústeres	Read			
DescribeDataSharesForProducer	Concede permiso para describir solo el recurso compartido de datos creado por los clústeres	Read			
DescribeDefaultClusterParameters	Concede permiso para describir la configuración de parámetros para una familia de grupos de parámetros	Lectura			
DescribeEndpointAccess	Concede permiso para describir los puntos de conexión de VPC administrados por redshift	Lectura			
DescribeEndpointAuthorization	Concede permiso para autorizar la actividad de descripción para un punto de conexión de VPC administrado por redshift	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeEventCategories	Concede permiso para describir las categorías de eventos para todos los tipos de orígenes de eventos o para un tipo de origen especificado	Lectura			
DescribeEventSubscriptions	Otorga permiso para describir las suscripciones a notificaciones de eventos de Amazon Redshift para las suscripciones especificadas Cuenta de AWS	Lectura			
DescribeEvents	Concede permiso para describir los eventos relacionados con los clústeres, los grupos de seguridad, las instantáneas y los grupos de parámetros de los últimos 14 días	List			
DescribeHsmClientCertificates	Concede permiso para describir los certificados del cliente de HSM	Read			
DescribeHsmConfigurations	Concede permiso para describir las configuraciones de HSM de Amazon Redshift	Lectura			
DescribeInboundIntegrations	Concede permiso para enumerar las integraciones entrantes	Enumeración		redshift:InboundIntegrationArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeIntegrations	Concede permiso para describir una integración sin ETL de Amazon Redshift	Enumeración	integration*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingStatus	Concede permiso para describir si se está registrando información, como consultas e intentos de conexión, para un clúster	Read	cluster*		
DescribeNodeConfigurationOptions	Concede permiso para describir las propiedades de posibles configuraciones de nodo, como el tipo de nodo, el número de nodos y el uso del disco para el tipo de acción especificado	List			
DescribeOrderableClusterOptions	Concede permiso para describir las opciones del clúster que se pueden ordenar	Lectura			
DescribePartners	Concede permiso para recuperar información sobre las integraciones de socios definidas para un clúster	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeQev2IdcApplications [solo permiso]	Concede permiso para describir aplicaciones QEV2 IDC	Enumeración			
DescribeQuery [solo permiso]	Concede permiso para describir una consulta a través de la consola de Amazon Redshift	Lectura			
DescribeRedshiftIdcApplications	Concede el permiso para describir aplicaciones redshift idc	Enumeración			sso:GetApplicationGrant sso:ListApplicationAccessScopes
DescribeReservedNodeExchangeStatus	Concede permiso para describir los detalles del estado de intercambio y los metadatos asociados para un intercambio de nodos reservados. Los estados incluyen valores tales como en curso y solicitado	Lectura			
DescribeReservedNodeOfferings	Concede permiso para describir las ofertas de nodos reservados disponibles en Amazon Redshift	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReservedNodes	Concede permiso para describir los nodos reservados	Read			
DescribeResize	Concede permiso para describir la última operación de cambio de tamaño de un clúster	Read	cluster*		
DescribeSavedQueries [solo permiso]	Concede permiso para describir las consultas guardadas a través de la consola de Amazon Redshift	Read			
DescribeScheduledActions	Concede permiso para describir las acciones programadas de Amazon Redshift creadas	Lectura			
DescribeSnapshotCopyGrants	Otorga permiso para describir las concesiones de copias instantáneas propiedad de la persona especificada Cuenta de AWS en el destino Región de AWS	Lectura			
DescribeSnapshotSchedules	Concede permiso para describir programaciones de instantáneas	Read	snapshotschedule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeStorage	Concede permiso para describir el tamaño de almacenamiento y el almacenamiento provisional de las copias de seguridad de nivel de cuenta	Read			
DescribeTable [solo permiso]	Concede permiso para describir una tabla a través de la consola de Amazon Redshift	Lectura			
DescribeTableRestoreStatus	Otorga permiso para describir el estado de una o más solicitudes de restauración de tablas realizadas mediante la acción de la RestoreTableFromClusterSnapshot API	Lectura			
DescribeTags	Concede permiso para describir etiquetas	Read	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			parameter group		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
DescribeUsageLimits	Concede permiso para describir los límites de uso	Read	usagelimit*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableLogging	Concede permiso para desactivar el registro de información, como consultas e intentos de conexión, para un clúster	Write	cluster*		
DisableSnapshotCopy	Concede permiso para desactivar la copia automática de instantáneas de un clúster	Write	cluster*		
DisassociateDataShareConsumer	Concede permiso para anular la asociación de un consumidor al recurso compartido de datos	Write	datashare*		
				redshift:ConsumerArn	
EnableLogging	Concede permiso para habilitar el registro de información, como consultas e intentos de conexión, para un clúster	Write	cluster*		
EnableSnapshotCopy	Concede permiso para habilitar la copia automática de instantáneas para un clúster	Write	cluster*		
ExecuteQuery [solo permiso]	Concede permiso para ejecutar una consulta a través de la consola de Amazon Redshift	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
FailoverPrimaryCompute	Concede permiso para realizar la conmutación por error del procesamiento principal de un clúster Multi-AZ a otra AZ	Escritura	cluster*		
FetchResults [solo permiso]	Concede permiso para obtener resultados de consulta a través de la consola de Amazon Redshift	Lectura			
GetClusterCredentials	Otorga permiso para obtener credenciales temporales para acceder a una base de datos de Amazon Redshift según lo especificado Cuenta de AWS	Escritura	dbuser*		
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	
GetClusterCredentialsWithIAM	Otorga permiso para obtener credenciales temporales mejoradas para acceder a una base de datos de Amazon Redshift según lo especificado Cuenta de AWS	Escritura	dbname		
				redshift:DbName redshift:DurationSeconds	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetReservedNodeExchangeConfigurationOptions	Concede permiso para obtener las opciones de configuración para el intercambio de nodos reservados	Lectura			
GetReservedNodeExchangeOfferings	Otorga permiso para obtener una matriz DC2 ReservedNodeOfferings que coincida con el tipo de pago, el plazo y el precio de uso del nodo DC1 reservado en cuestión	Lectura			
GetResourcePolicy	Concede permiso para obtener la política de recursos para un recurso especificado	Lectura	namespace*		
JoinGroup	Concede permiso para unirse al grupo especificado de Amazon Redshift	Permissions management	dbgroup*		
ListDatabases [solo permiso]	Concede permiso para mostrar bases de datos a través de la consola de Amazon Redshift	Enumeración			
ListRecommendations	Concede permiso para enumerar recomendaciones de Advisor	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSavedQueries [solo permiso]	Concede permiso para mostrar las consultas guardadas a través de la consola de Amazon Redshift	List			
ListSchemas [solo permiso]	Concede permiso para mostrar esquemas a través de la consola de Amazon Redshift	List			
ListTables [solo permiso]	Concede permiso para mostrar tablas a través de la consola de Amazon Redshift	List			
ModifyAquaConfiguration	Concede permiso para modificar la configuración de AQUA de un clúster	Escritura	cluster*		
ModifyAuthenticationProfile	Concede permiso para modificar un perfil de autenticación de Amazon Redshift existente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyCluster	Concede permiso para modificar la configuración de un clúster	Write	cluster*		acm:DescribeCertificate kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
ModifyClusterDbRevision	Concede permiso para modificar la revisión de la base de datos de un clúster	Escritura	cluster*		
ModifyClusterIamRoles	Otorga permiso para modificar la lista de funciones de AWS Identity and Access Management (IAM) que un clúster puede usar para acceder a otros servicios AWS	Administración de permisos	cluster*		
ModifyClusterMaintenance	Concede permiso para modificar la configuración de mantenimiento de un clúster	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyClusterParameterGroup	Concede permiso para modificar los parámetros de un grupo de parámetros	Write	parametergroup*		
ModifyClusterSnapshot	Concede permiso para modificar la configuración de una instantánea	Write	snapshot*		
ModifyClusterSnapshotSchedule	Concede permiso para modificar una programación de instantáneas para un clúster	Write	cluster*		
ModifyClusterSubnetGroup	Concede permiso para modificar un grupo de subredes del clúster para incluir la lista especificada de subredes de VPC	Escritura	subnetgroup*		
ModifyCustomDomainAssociation	Otorga permiso para modificar un nombre de dominio personalizado para un clúster	Escritura	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	Concede permiso para modificar un punto de conexión de VPC administrado por redshift	Escritura			
ModifyEventSubscription	Concede permiso para modificar una suscripción de notificación de eventos de Amazon Redshift existente	Escritura	eventsubscription*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyIntegration	Concede permiso para modificar una integración sin ETL de Amazon Redshift	Escritura	integration*		
				aws:ResourceTag/${TagKey}	
ModifyQev2IdcApplication [solo permiso]	Concede permiso para modificar una aplicación QEV2 IDC	Escritura	qev2idcapplication*		sso:UpdateApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyRedshiftIdcApplication	Concede permiso para modificar una aplicación redshift idc	Escritura	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifySavedQuery [solo permiso]	Concede permiso para modificar una consulta guardada existente a través de la consola de Amazon Redshift	Write			
ModifyScheduledAction	Concede permiso para modificar una acción programada de Amazon Redshift existente	Escritura			
ModifySnapshotCopyRetentionPeriod	Otorga permiso para modificar el número de días para conservar las instantáneas en el destino una Región de AWS vez que se hayan copiado de la fuente Región de AWS	Escritura	cluster*		
ModifySnapshotSchedule	Concede permiso para modificar una programación de instantáneas	Write	snapshotschedule*		
ModifyUsageLimit	Concede permiso para modificar un límite de uso	Write	usagelimit*		
PauseCluster	Concede permiso para pausar un clúster	Write	cluster*		
PurchaseReservedNodeOffering	Concede permiso para comprar un nodo reservado	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResourcePolicy	Concede permiso para actualizar una política de recursos para un recurso especificado	Administración de permisos	namespace*		
RebootCluster	Concede permiso para reiniciar un clúster	Escritura	cluster*		
RegisterNamespace	Otorga permiso a un consumidor para registrar el espacio de nombres especificado	Escritura			
RejectDataShare	Concede permiso para rechazar un recurso compartido de datos de otra cuenta	Permissions management	datashare*		
ResetClusterParameterGroup	Concede permiso para establecer uno o varios parámetros del grupo de parámetros especificado en sus valores predeterminados y establecer los valores de origen de los parámetros en "engine-default"	Write	parametergroup*		
ResizeCluster	Concede permiso para cambiar el tamaño de un clúster	Write	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreFromClusterSnapshot	Concede permiso para crear un clúster a partir de una instantánea	Write	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
			snapshot*		
				aws:TagKeys	
RestoreTableFromClusterSnapshot	Concede permiso para crear una tabla a partir de una tabla en una instantánea de clúster de Amazon Redshift	Write	cluster*		
			snapshot*		
ResumeCluster	Concede permiso para reanudar un clúster	Escritura	cluster*		
RevokeClusterSecurityGroupIngress	Otorga permiso para revocar una regla de entrada en un grupo de seguridad de Amazon Redshift para un rango de IP o un grupo de seguridad de Amazon previamente autorizados EC2	Escritura	securitygroup*		
			securitygroupingress-ec2securitygroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RevokeEndpointAccess	Concede permiso para revocar el acceso para actividades relacionadas con puntos de conexión para puntos de conexión de VPC administrados por redshift	Administración de permisos			
RevokeSnapshotAccess	Otorga permiso para revocar el acceso de la persona especificada Cuenta de AWS con el fin de restaurar una instantánea	Administración de permisos	snapshot*		
RotateEncryptionKey	Concede permiso para rotar una clave de cifrado para un clúster	Escritura	cluster*		
UpdatePartnerStatus	Concede permiso para actualizar el estado de una integración de socios	Escritura			
ViewQueriesFromConsole [solo permiso]	Concede permiso para ver los resultados de la consulta a través de la consola de Amazon Redshift	List			
ViewQueriesInConsole [solo permiso]	Concede permiso para terminar las consultas y cargas en ejecución a través de la consola de Amazon Redshift	List			

Tipos de recursos definidos por Amazon Redshift

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
datashare	`arn:${Partition}:redshift:${Region}:${Account}:datashare:${ProducerClusterNamespace}/${DataShareName}`	aws:ResourceTag/${TagKey}
dbgroup	`arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}`	
dbname	`arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}`	
dbuser	`arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}`	
eventsubscription	`arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}`	aws:ResourceTag/${TagKey}
hsmclientcertificate	`arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
hsmconfiguration	arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:redshift:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:redshift:${Region}:${Account}:namespace:${ClusterNamespace}	aws:ResourceTag/${TagKey}
parametergroup	arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}	aws:ResourceTag/${TagKey}
securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}	aws:ResourceTag/${TagKey}
securitygroupingress-cidr	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}	aws:ResourceTag/${TagKey}
securitygroupingress-ec2securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
snapshotcopygrant	arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}	aws:ResourceTag/${TagKey}
snapshotschedule	arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ScheduleIdentifier}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}	aws:ResourceTag/${TagKey}
usagelimit	arn:${Partition}:redshift:${Region}:${Account}:usagelimit:${UsageLimitId}	aws:ResourceTag/${TagKey}
redshiftidcapplication	arn:${Partition}:redshift:${Region}:${Account}:redshiftidcapplication:${RedshiftIdcApplicationId}	
qev2idcapplication	arn:${Partition}:redshift:${Region}:${Account}:qev2idcapplication:${Qev2IdcApplicationId}	

Claves de condición de Amazon Redshift

Amazon Redshift define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por acciones en función del conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por acciones en función del valor de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra accesos en función de la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
redshift:AllowWrites	Filtra el acceso por el parámetro de entrada allowWrites	Bool
redshift:ConsumerArn	Filtra el acceso por el ARN de consumidor del recurso compartido de datos.	ARN
redshift:ConsumerIdentifier	Filtra el acceso por el consumidor del recurso compartido de datos	Cadena
redshift:DbName	Filtra el acceso por el nombre de la base de datos.	Cadena
redshift:DbUser	Filtra el acceso por el nombre de usuario de la base de datos.	Cadena
redshift:DurationSeconds	Filtra el acceso por el número de segundos hasta que caduca un conjunto de credenciales temporales.	Cadena
redshift:InboundIntegrationArn	Filtra el acceso por el ARN de un recurso de integración sin ETL entrante	ARN
redshift:IntegrationSourceArn	Filtra el acceso por el ARN de un origen de integración sin ETL	ARN

Claves de condición	Descripción	Tipo
redshift:IntegrationTargetArn	Filtra el acceso por el ARN de un destino de integración sin ETL	ARN

Acciones, recursos y claves de condición para la API de datos de Amazon Redshift

La API de datos de Amazon Redshift (prefijo de servicio: `redshift-data`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la API de datos de Amazon Redshift
- Tipos de recurso definidos por la API de datos de Amazon Redshift
- Claves de condición de la API de datos de Amazon Redshift

Acciones definidas por la API de datos de Amazon Redshift

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchExecuteStatement	Concede permiso para ejecutar varias consultas bajo una sola conexión	Escritura	cluster		
			workgroup		
				redshift-data:session-owner-iam-userid	
				redshift-data:glue-catalog-arn	
CancelStatement	Concede permiso para cancelar una consulta en ejecución	Write		redshift-data:statement-owner-iam-userid	
DescribeStatement	Concede permiso para recuperar información detallada sobre la ejecución de una sentencia	Read		redshift-data:statement-owner-iam-userid	
DescribeTable	Concede permiso para recuperar metadatos sobre una tabla concreta	Read	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workgroup*		
ExecuteStatement	Concede permiso para ejecutar una consulta	Escritura	cluster		
			workgroup		
				redshift-data:session-owner-iam-userid redshift-data:glue-catalog-arn	
GetStagingBucketLocation	Otorga permiso para obtener la ubicación del depósito provisional para un grupo de trabajo administrado determinado	Lectura	managed-workgroup*		
GetStatementResult	Concede permiso para obtener el resultado de una consulta	Read		redshift-data:statement-owner-iam-userid	
ListDatabases		Read	cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para enumerar bases de datos para un clúster determinado		workgroup*		
ListSchemas	Concede permiso para enumerar esquemas de un clúster determinado	Read	cluster*		
			workgroup*		
ListStatements	Concede permiso para enumerar consultas para una entidad principal determinada	List		redshift-data:statement-owner-iam-userid	
ListTables	Concede permiso para enumerar tablas de un clúster determinado	List	cluster*		
			workgroup*		

Tipos de recurso definidos por la API de datos de Amazon Redshift

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}	aws:ResourceTag/${TagKey}
workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}	aws:ResourceTag/${TagKey}
managed-workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupId}	

Claves de condición de la API de datos de Amazon Redshift

La API de datos de Amazon Redshift define las siguientes claves de condición que pueden usarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
redshift-data:glue-catalog-arn	Filtra el acceso por barra de catálogo azul	ARN
redshift-data:session-	Filtra el acceso por el ID de usuario de IAM del propietario de la sesión	Cadena

Claves de condición	Descripción	Tipo
owner-iam-user id		
redshift-data:statement-owner-iam-us erid	Filtra el acceso por el propietario de la instrucción iam userid	Cadena

Acciones, recursos y claves de condición para Amazon Redshift sin servidor

Amazon Redshift sin servidor (prefijo de servicio: `redshift-serverless`) proporciona los siguientes recursos específicos del servicio, acciones y claves de contexto de condición para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Redshift sin servidor
- Tipos de recursos definidos por Amazon Redshift sin servidor
- Claves de condición de Amazon Redshift sin servidor

Acciones definidas por Amazon Redshift sin servidor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ConvertRecoveryPointToSnapshot	Otorga permiso para convertir un punto de recuperación en una instantánea.	Escritura	recoveryPoint*		
			snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDomainAssociation	Otorga permiso para crear una asociación de dominio personalizado en Amazon Redshift sin servidor.	Escritura	workgroup*		acm:DescribeCertificate
CreateEndpointAccess	Concede permiso para crear un punto de conexión de VPC administrado por Amazon Redshift sin servidor	Escritura	endpointAccess*		
CreateNamespace	Otorga permiso para crear un espacio de nombres de Amazon Redshift sin servidor.	Escritura	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservation	Otorga permiso para comprar una reserva de capacidad de acuerdo con una oferta de reserva específica, para un número específico de RPUs	Escritura			
CreateScheduledAction	Concede permiso para crear una acción programa para un espacio de nombres de Amazon Redshift sin servidor específico	Escritura	namespace*		
CreateSnapshot	Otorga permiso para crear una instantánea de todas las bases de datos en un espacio de nombres.	Escritura	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSnapshotCopyConfiguration	Concede permiso para crear una configuración de copia de instantáneas para un espacio de nombres de Amazon Redshift sin servidor específico	Escritura	namespace*		
CreateUsageLimit	Otorga permiso para crear un límite de uso para un tipo de uso de Amazon Redshift sin servidor específico.	Escritura			
CreateWorkgroup	Otorga permiso para crear un grupo de trabajo en Amazon Redshift sin servidor.	Escritura	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomDomainAssociation	Otorga permiso para eliminar una asociación de dominio personalizada	Escritura	workgroup*		
DeleteEndpointAccess	Otorga permiso para eliminar un punto de conexión de VPC administrado por Amazon Redshift sin servidor	Escritura	endpointAccess*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteNamespace	Otorga permiso para eliminar un espacio de nombres de Amazon Redshift sin servidor.	Escritura	namespace*		kms:DescribeKey kms:RetireGrant secretsmanager:DeleteSecret secretsmanager:DescribeSecret
DeleteResourcePolicy	Otorga permiso para eliminar la política de recursos especificada.	Escritura			
DeleteScheduledAction	Concede permiso para eliminar una acción programada de Amazon Redshift sin servidor	Escritura			
DeleteSnapshot	Otorga permiso para eliminar una instantánea de Amazon Redshift sin servidor.	Escritura	snapshot*		
DeleteSnapshotCopyConfiguration	Concede permiso para eliminar una configuración de copia de instantáneas para un espacio de nombres de Amazon Redshift sin servidor	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUsageLimit	Otorga permiso para eliminar un límite de uso de Amazon Redshift sin servidor.	Escritura			
DeleteWorkgroup	Concede permiso para eliminar un grupo de trabajo	Escritura	workgroup*		
DescribeOneTimeCredit [solo permiso]	Concede permiso para ver en la consola de Amazon Redshift sin servidor el número restante de créditos de prueba gratuita y su fecha de caducidad	Lectura			
GetCredentials	Concede permiso para obtener un nombre de usuario y una contraseña temporal de la base de datos con autorización temporal para iniciar sesión en Amazon Redshift sin servidor.	Escritura	workgroup*		
GetCustomDomainAssociation	Concede permisos para ver información sobre una asociación de dominio personalizado específica	Lectura	workgroup*		
GetEndpointAccess	Concede permiso para crear un punto de conexión de VPC administrado por Amazon Redshift sin servidor	Lectura	endpointAccess*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetManagedWorkgroup	Otorga permiso para crear un grupo de trabajo sin servidor gestionado por Amazon Redshift con los ajustes de configuración especificados	Lectura	managed-workgroup*		
GetNamespace	Otorga permiso para obtener información sobre un espacio de nombres en Amazon Redshift sin servidor.	Lectura	namespace*		
GetRecoveryPoint	Otorga permiso para obtener información sobre un punto de recuperación.	Lectura	recoveryPoint*		
GetReservation	Otorga permiso para obtener un objeto de reserva concreto	Lectura			
GetReservationOffering	Otorga permiso para obtener una oferta de reserva concreta	Lectura			
GetResourcePolicy	Otorga permiso para obtener una política de recursos.	Lectura			
GetScheduledAction	Concede permiso para obtener información sobre una acción programada específica	Lectura			
GetSnapshot	Otorga permiso para obtener información sobre una instantánea específica.	Lectura	snapshot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTableRestoreStatus	Concede permiso para obtener el estado de restauración de tabla de una instantánea específica	Lectura			
GetTrack	Otorga permiso para obtener información sobre una pista en Amazon Redshift Serverless	Lectura			
GetUsageLimit	Otorga permiso para obtener información sobre un límite de uso en Amazon Redshift sin servidor.	Lectura			
GetWorkgroup	Otorga permiso para obtener información acerca de un grupo de trabajo específico.	Lectura	workgroup*		
ListCustomDomainAssociations	Otorga permiso para mostrar asociaciones de dominio personalizadas en Amazon Redshift sin servidor.	Enumeración			
ListEndpointAccess	Otorga permiso para enumerar EndpointAccess objetos e información relevante	Enumeración	endpointAccess*		
ListManagedWorkgroups	Otorga permiso para enumerar los grupos de trabajo administrados en Amazon Redshift Serverless	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNamespaces	Otorga permiso para mostrar los espacios de nombres en Amazon Redshift sin servidor.	Enumeración			
ListRecoveryPoints	Otorga permiso para obtener una matriz de puntos de recuperación.	Enumeración	namespace		
ListReservationOfferings	Otorga permiso para enumerar todas las ofertas de reserva de capacidad disponibles	Enumeración			
ListReservations	Otorga permiso para publicar todas las reservas	Enumeración			
ListScheduledActions	Concede permiso para enumerar acciones programadas	Enumeración			
ListSnapshotCopyConfigurations	Otorga permiso para enumerar SnapshotCopyConfiguration objetos e información relevante	Enumeración	namespace		
ListSnapshots	Otorga permiso para enumerar instantáneas.	Enumeración	snapshot*		
ListTableRestoreStatus	Concede permiso para enumerar el estado de restauración de tabla	Enumeración			
ListTagsForResource		Enumeración	namespace		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para enumerar las etiquetas asignadas a un recurso.		workgroup		
				aws:ResourceTag/${TagKey}	
ListTracks	Otorga permiso para enumerar las pistas disponibles en Amazon Redshift Serverless	Enumeración			
ListUsageLimits	Otorga permiso para mostrar todos los límites de uso en Amazon Redshift sin servidor.	Enumeración			
ListWorkgroups	Otorga permiso para mostrar grupos de trabajo en Amazon Redshift sin servidor.	Enumeración			
PutResourcePolicy	Concede permiso para crear o actualizar una política de recursos	Escritura			
RestoreFromRecoveryPoint	Otorga permiso para restaurar los datos a partir desde un punto de recuperación.	Escritura	recoveryPoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreFromSnapshot	Otorga permiso para restaurar el espacio de nombres a partir de una instantánea.	Escritura	snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
RestoreTableFromRecoveryPoint	Concede permiso para restaurar una tabla a partir de un punto de recuperación	Escritura	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	Concede permiso para restaurar una tabla a partir de una instantánea	Escritura	namespace*		
			snapshot*		
TagResource	Otorga permiso para asignar una o varias etiquetas a un recurso.	Etiquetado	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una etiqueta o conjunto de etiquetas de un recurso.	Etiquetado	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateCustomDomainAssociation	Otorga permiso para actualizar un certificado asociado a un dominio personalizado	Escritura	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	Concede permiso para actualizar un punto de conexión de VPC administrado por Amazon Redshift sin servidor	Escritura	endpointAccess*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateNamespace	Otorga permiso para actualizar un espacio de nombres con los valores de configuración especificados.	Escritura	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
UpdateScheduledAction	Concede permiso para actualizar una acción programada	Escritura			
UpdateSnapshot	Otorga permiso para actualizar una instantánea.	Escritura	snapshot*		
UpdateSnapshotCopyConfiguration	Concede permiso para actualizar una configuración de copia de instantáneas para un espacio de nombres de Amazon Redshift sin servidor	Escritura			
UpdateUsageLimit	Otorga permiso para actualizar un límite de uso en Amazon Redshift sin servidor.	Escritura			
UpdateWorkgroup	Otorga permiso para actualizar un grupo de trabajo sin servidor de Amazon Redshift sin servidor con los valores de configuración especificados.	Escritura	workgroup*		

Tipos de recursos definidos por Amazon Redshift sin servidor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
namespace	`arn:${Partition}:redshift-serverless:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:redshift-serverless:${Region}:${Account}:snapshot/${SnapshotId}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}
managed-workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupName}`	
recoveryPoint	`arn:${Partition}:redshift-serverless:${Region}:${Account}:recoverypoint/${RecoveryPointId}`	aws:ResourceTag/${TagKey}
endpointAccess	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managedvpcendpoint/${EndpointAccessId}`	

Claves de condición de Amazon Redshift sin servidor

Amazon Redshift sin servidor define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
redshift-serverless:endpointAccessId	Filtra el acceso mediante el identificador de acceso del punto de conexión.	Cadena
redshift-serverless:managedWorkgroupName	Filtra el acceso por el identificador del grupo de trabajo gestionado	Cadena
redshift-serverless:namespaceId	Filtra el acceso mediante el identificador del espacio de nombres.	Cadena
redshift-serverles	Filtra el acceso mediante el identificador del punto de recuperación.	Cadena

Claves de condición	Descripción	Tipo
s:recoveryPointId		
redshift-serverless:snapshotId	Filtra el acceso mediante el identificador de la instantánea.	Cadena
redshift-serverless:tableRestoreRequestId	Filtra el acceso mediante el identificador de la solicitud de restauración de tabla	Cadena
redshift-serverless:workgroupId	Filtra el acceso mediante el identificador del grupo de trabajo.	Cadena

Acciones, recursos y claves de condición de Amazon Rekognition

Amazon Rekognition (prefijo de servicio: `rekognition`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Rekognition
- Tipos de recurso definidos por Amazon Rekognition
- Claves de condición de Amazon Rekognition

Acciones definidas por Amazon Rekognition

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateFaces	Concede permiso para asociar varios rostros individuales a un solo usuario	Escritura	collection*		
CompareFaces	Concede permiso para comparar los rostros de la imagen de entrada de origen con cada rostro detectado en la imagen de entrada de destino	Lectura			
CopyProjectVersion	Concede permiso para copiar una versión del modelo existente en una nueva versión del modelo.	Escritura	project*		
			projectversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCollection	Otorga permiso para crear una colección en un Región de AWS	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataset	Otorga permiso para crear un nuevo conjunto de datos de etiquetas personalizadas de Amazon Rekognition.	Escritura	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFaceLivenessSession	Concede permiso para crear una sesión de prueba de vida	Escritura			
CreateProject	Otorga permiso para crear un proyecto de etiquetas personalizadas de Amazon Rekognition.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProjectVersion	Otorga permiso para comenzar a entrenar una nueva versión de un modelo.	Escritura	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamProcessor	Otorga permiso para crear un procesador de transmisión de Amazon Rekognition.	Escritura	collection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Concede permiso para crear un nuevo usuario en una colección con un ID de usuario único que usted proporcione	Escritura	collection*		
DeleteCollection	Otorga permiso para eliminar la colección especificada.	Escritura	collection*		
DeleteDataset	Otorga permiso para eliminar un conjunto de datos existente de etiquetas personalizadas de Amazon Rekognition.	Escritura	dataset*		
DeleteFaces	Otorga permiso para eliminar rostros de una colección.	Escritura	collection*		
DeleteProject	Concede permiso para eliminar un proyecto	Escritura	project*		
DeleteProjectPolicy	Concede permiso para eliminar la política de recursos adjunta a un proyecto.	Escritura	project*		
DeleteProjectVersion	Concede permiso para eliminar un modelo	Escritura	projectversion*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteStreamProcessor	Otorga permiso para eliminar el procesador de transmisión especificado.	Escritura	streamprocessor*		
DeleteUser	Concede permiso para eliminar un usuario de una colección en función del ID de usuario proporcionado	Escritura	collection*		
DescribeCollection	Otorga permiso para leer detalles acerca de una colección.	Lectura	collection*		
DescribeDataset	Otorga permiso para describir un conjunto de datos de etiquetas personalizadas de Amazon Rekognition.	Lectura	dataset*		
DescribeProjectVersions	Otorga permiso para enumerar las versiones de un modelo en un proyecto de etiquetas personalizadas de Amazon Rekognition.	Lectura	project*		
DescribeProjects	Otorga permiso para enumerar los proyectos de etiquetas personalizadas de Amazon Rekognition.	Lectura			
DescribeStreamProcessor	Otorga permiso para obtener información acerca del procesador de transmisión especificado.	Lectura	streamprocessor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DetectCustomLabels	Otorga permiso para detectar etiquetas personalizadas en una imagen suministrada.	Lectura	projectversion*		
DetectFaces	Otorga permiso para detectar rostros humanos en una imagen proporcionada como entrada.	Lectura			
DetectLabels	Otorga permiso para detectar instancias de etiquetas del mundo real dentro de una imagen proporcionada como entrada.	Lectura			
DetectModerationLabels	Otorga permiso para detectar etiquetas de moderació n dentro de la imagen de entrada,	Lectura	projectversion		
DetectProtectiveEquipment	Otorga permiso para detectar el equipo de protección personal en la imagen de entrada.	Lectura			
DetectText	Otorga permiso para detectar texto en la imagen de entrada y lo convierte en texto legible por una máquina.	Lectura			
DisassociateFaces	Concede permiso para eliminar la asociación entre un ID de usuario y un ID de rostro	Escritura	collection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DistributeDatasetEntries	Otorga permiso para distribuir las entradas de un conjunto de datos de formación en todo el conjunto de datos de formación y el conjunto de datos de prueba de un proyecto.	Escritura	dataset*		
GetCelebrityInfo	Otorga permiso para leer el nombre y la información adicional de una celebridad.	Lectura			
GetCelebrityRecognition	Otorga permiso para leer los resultados de reconocimiento de celebridades encontrados en un video almacenado por un trabajo de reconocimiento de celebridades asíncrono.	Lectura			
GetContentModeration	Otorga permiso para leer los resultados del análisis de moderación de contenido que se encuentran en un video almacenado mediante un trabajo de moderación de contenido asíncrono.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFaceDetection	Otorga permiso para leer los resultados de detección de rostros encontrados en un video almacenado mediante un trabajo de detección de rostros asíncrono.	Lectura			
GetFaceLivenessSessionResults	Concede permiso para obtener los resultados de una sesión de prueba de vida	Lectura			
GetFaceSearch	Otorga permiso para leer los rostros coincidentes de la colección encontrados en un video almacenado mediante un trabajo de búsqueda asíncrona de rostros.	Lectura			
GetLabelDetection	Otorga permiso para leer los resultados de la etiqueta detectados en un video almacenado mediante un trabajo de detección de etiquetas asíncrono.	Lectura			
GetMediaAnalysisJob	Otorga permiso para leer la referencia a los resultados del trabajo en S3 y la información adicional sobre un trabajo de análisis de medios	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPersonTracking	Otorga permiso para leer la lista de personas detectadas en un video almacenado por un trabajo de seguimiento de personas asíncrono.	Lectura			
GetSegmentDetection	Otorga permiso para obtener los segmentos de video que se encuentran en un video almacenado mediante un trabajo de detección de segmentos asíncrono.	Lectura			
GetTextDetection	Otorga permiso para obtener el texto encontrado en un video almacenado mediante un trabajo de detección de texto asíncrono.	Lectura			
IndexFaces	Otorga permiso para actualizar una colección existente con rostros detectados en la imagen de entrada.	Escritura	collection*		
ListCollections	Otorga permiso para leer los ID de colección de su cuenta.	Lectura			
ListDatasetEntries	Otorga permiso para enumerar las entradas del conjunto de datos en un conjunto de datos de etiquetas personalizadas de Amazon Rekognition existente.	Lectura	dataset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDatasetLabels	Otorga permiso para enumerar todas las etiquetas en un conjunto de datos.	Lectura	dataset*		
ListFaces	Otorga permiso para leer metadatos de los rostros de la colección especificada.	Lectura	collection*		
ListMediaAnalysisJobs	Otorga permiso para leer la lista de trabajos de análisis de medios	Lectura			
ListProjectPolicies	Concede permiso para enumerar la política de recursos asociada a un proyecto.	Lectura	project*		
ListStreamProcessors	Otorga permiso para obtener una lista de sus procesadores de streaming.	Enumeración			
ListTagsForResource	Otorga permiso para devolver una lista de etiquetas asociadas a un recurso.	Lectura	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListUsers	Otorga permiso para enumerar UserIds y UserStatus	Lectura	collection*		
PutProjectPolicy	Concede permiso para adjuntar una política de recursos a un proyecto.	Escritura	project*		
RecognizeCelebrities	Otorga permiso para detectar celebridades en la imagen de entrada.	Lectura			
SearchFaces	Otorga permiso para buscar en la colección especificada el ID de rostro suministrado.	Lectura	collection*		
SearchFacesByImage	Otorga permiso para buscar en la colección especificada el rostro más grande de la imagen de entrada.	Lectura	collection*		
SearchUsers	Concede permiso para buscar en la colección especificada el resultado de coincidencias de usuarios con el ID de rostro o ID de usuario proporcionado	Lectura	collection*		
SearchUsersByImage	Concede permiso para buscar en la colección especificada el resultado de coincidencias de usuarios mediante el rostro más grande de la imagen de entrada	Lectura	collection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCelebrityRecognition	Otorga permiso para iniciar el reconocimiento asincrónico de famosos en un vídeo almacenado	Escritura			
StartContentModeration	Otorga permiso para iniciar la detección asincrónica de contenido explícito o sugerente para adultos en un video.	Escritura			
StartFaceDetection	Otorga permiso para iniciar la detección asincrónica de rostros en un video almacenado.	Escritura			
StartFaceLivenessSession	Concede permiso para iniciar la transmisión de vídeo para una sesión de prueba de vida	Escritura			
StartFaceSearch	Otorga permiso para iniciarla búsqueda asincrónica de rostros en una colección que coincidan con los rostros de las personas detectadas en un video.	Escritura	collection*		
StartLabelDetection	Otorga permiso para iniciar la detección asincrónica de etiquetas en un vídeo almacenado.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartMediaAnalysisJob	Concede permiso para comenzar un trabajo de análisis de medios	Escritura	projectversion		
StartPersonTracking	Otorga permiso para iniciar el seguimiento asincrónico de personas en un vídeo almacenado.	Escritura			
StartProjectVersion	Otorga permiso para iniciar a ejecutar una versión de un modelo.	Escritura	projectversion*		
StartSegmentDetection	Otorga permiso para iniciarla detección asincrónica de segmentos en un video almacenado.	Escritura			
StartStreamProcessor	Otorga permiso para iniciar la ejecución de un procesador de secuencia.	Escritura	streamprocessor*		
StartTextDetection	Otorga permiso para iniciar la detección asincrónica del texto en un video almacenado	Escritura			
StopProjectVersion	Otorga permiso para detener una versión de modelo en ejecución.	Escritura	projectversion*		
StopStreamProcessor	Otorga permiso para detener un procesador de secuencia en ejecución.	Escritura	streamprocessor*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso.	Etiquetado	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDatasetEntries	Otorga permiso para agregar o actualizar una o más líneas JSON (entradas) en un conjunto de datos.	Escritura	dataset*		
UpdateStreamProcessor	Otorga permiso para modificar las propiedades de un procesador de flujo.	Escritura	streamprocessor*		

Tipos de recurso definidos por Amazon Rekognition

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
collection	`arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
streamprocessor	`arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
projectversion	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/dataset/${DatasetType}/${CreationTimestamp}	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Rekognition

Amazon Rekognition define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de acción, recursos y condición de AWS RePost Private

AWS RePost Private (prefijo de servicio:`repostspace`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por RePost Private AWS
- Tipos de recursos definidos por RePost Private AWS
- Claves de condición para AWS RePost Private

Acciones definidas por RePost Private AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchAddRole	Otorga permiso para añadir un rol a los usuarios y grupos de una cuenta privada de Re:post	Escritura	space*		
BatchRemoveRole	Otorga permiso para eliminar un rol de los usuarios y grupos de un Re:post privado de tu cuenta	Escritura	space*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSpace	Concede permiso para crear un nuevo re:Post privado en su cuenta	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteSpace	Concede permiso para eliminar un re:Post privado de su cuenta	Escritura	space*		
DeregisterAdmin	Conceda permiso para eliminar a un administrador de un re:Post privado de su cuenta	Escritura	space*		
GetSpace	Concede permiso para obtener la descripción de un re:Post privado en su cuenta	Lectura	space*		
ListSpaces	Concede permiso para enumerar todos los re:Post privados de su cuenta	Lectura			
ListTagsForResource	Otorga permiso para enumerar las etiquetas asociadas a un recurso.	Lectura	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterAdmin	Otorga permiso para añadir un administrador a un Re:post privado de tu cuenta	Escritura	space*		
SendInvites	Concede permiso para enviar invitaciones a los usuarios de un re:Post privado en su cuenta	Escritura	space*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	space*		
				aws:TagKeys	
UpdateSpace	Concede permiso para actualizar un re:Post en su cuenta	Escritura	space*		

Tipos de recursos definidos por RePost Private AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
space	`arn:${Partition}:repostspace:${Region}:${Account}:space/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS RePost Private

AWS RePost Private define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Resilience Hub

AWS Resilience Hub (prefijo de servicio:`resiliencehub`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Resilience Hub
- Tipos de recurso definidos por AWS Resilience Hub
- Claves de condición de AWS Resilience Hub

Acciones definidas por AWS Resilience Hub

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptResourceGroupingRecommendations	Concede permiso para aceptar recomendaciones de agrupamiento de recursos	Escritura	application*		
AddDraftAppVersionResourceMappings	Otorga permiso para agregar asignaciones de recursos de versión de la aplicación de borrador.	Escritura	application*		cloudformation:DescribeStacks cloudformation:ListStackResources

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
BatchUpdateRecommendationStatus	Concede permiso para incluir o excluir una o más recomendaciones operativas	Escritura	application*		
CreateApp	Otorga permiso para crear una aplicación.	Escritura	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAppVersionAppComponent	Otorga permiso para crear un componente de aplicación	Escritura	application*		
CreateAppVersionResource	Otorga permiso para crear un recurso de aplicación	Escritura	application*		
CreateRecommendationTemplate	Otorga permiso para crear una plantilla de recomendación.	Escritura	application*		s3:CreateBucket s3:ListBucket s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResiliencyPolicy	Otorga permiso para crear una política de resiliencia.	Escritura	resiliency-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApp	Otorga permiso para eliminar una aplicación por lotes.	Escritura	application*		
DeleteAppAssessment	Otorga permiso para eliminar la evaluación de aplicaciones por lotes.	Escritura	application*		
DeleteAppInputSource	Otorga permiso para eliminar la fuente de entrada de aplicación	Escritura	application*		
DeleteAppVersionAppComponent	Otorga permiso para eliminar un componente de aplicación	Escritura	application*		
DeleteAppVersionResource	Otorga permiso para eliminar un recurso de aplicación	Escritura	application*		
DeleteRecommendationTemplate	Otorga permiso para eliminar la plantilla de recomendación por lotes.	Escritura	application*		
DeleteResiliencyPolicy	Otorga permiso para eliminar una política de recursos por lotes.	Escritura	resiliency-policy*		
DescribeApp	Otorga el permiso para describir una aplicación.	Lectura	application*		
DescribeAppAssessment	Otorga permiso para describir una evaluación de aplicación.	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAppVersion	Otorga permiso para describir una versión de la aplicación	Lectura	application*		
DescribeAppVersionAppComponent	Otorga permiso para describir un componente de versión de una aplicación	Lectura	application*		
DescribeAppVersionResource	Otorga permiso para describir un recurso de versión de la aplicación	Lectura	application*		
DescribeAppVersionResourcesResolutionStatus	Otorga permiso para describir una resolución de aplicación.	Lectura	application*		
DescribeAppVersionTemplate	Otorga permiso para describir una plantilla de versión de la aplicación.	Lectura	application*		
DescribeDraftAppVersionResourcesImportStatus	Otorga permiso para describir el estado de importación de recursos de la versión de borrador de la aplicación.	Lectura	application*		
DescribeMetricsExport	Otorga permiso para describir la exportación de métricas	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeResiliencyPolicy	Otorga permiso para describir una política de resiliencia.	Lectura	resiliency-policy*		
DescribeResourceGroupingRecommendationTask	Concede permiso para describir el estado más reciente del proceso de recomendación de agrupamiento	Lectura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportResourcesToDraftAppVersion	Otorga permiso para importar recursos a la versión de borrador de la aplicación.	Escritura	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
ListAlarmRecommendations	Otorga permiso para enumerar una recomendación de alarma	Enumeración	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAppAssessmentComplianceDrifts	Concede permiso para enumerar las infracciones de cumplimiento que se detectaron al ejecutar una evaluación	Enumeración	application*		
ListAppAssessmentResourceDrifts	Concede permiso para enumerar las desviaciones de recursos que se detectaron durante la ejecución de una evaluación	Enumeración	application*		
ListAppAssessments	Otorga permiso para enumerar la evaluación de la aplicación.	Enumeración			
ListAppComponentCompliances	Otorga permiso para enumerar los componentes de una aplicación.	Enumeración	application*		
ListAppComponentRecommendations	Otorga permiso para enumerar recomendaciones de componentes de aplicación.	Enumeración	application*		
ListAppInputSources	Otorga permiso para enumerar los recursos de entrada de aplicación	Enumeración	application*		
ListAppVersionAppComponents	Otorga permiso para enumerar los componentes de versión de aplicación	Enumeración	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAppVersionResourceMappings	Otorga permiso a asignaciones de recursos de versiones de aplicaciones.	Enumeración	application*		
ListAppVersionResources	Otorga permiso para enumerar los recursos asociados a una aplicación.	Enumeración	application*		
ListAppVersions	Otorga permiso para enumerar las versiones de la aplicación.	Enumeración	application*		
ListApps	Otorga permiso para enumerar las aplicaciones.	Enumeración			
ListMetrics	Otorga permiso para enumerar las métricas	Enumeración			
ListRecommendationTemplates	Otorga permiso para enumerar las plantillas de recomendación.	Enumeración	application*		
ListResiliencyPolicies	Otorga permiso para enumerar las políticas de resiliencia.	Enumeración			
ListResourceGroupingRecommendations	Concede permiso para enumerar recomendaciones de agrupamiento de recursos	Enumeración	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSopRecommendations	Otorga permiso para enumerar recomendaciones de SOP.	Enumeración	application*		
ListSuggestedResiliencyPolicies	Otorga permiso para enumerar las políticas de resiliencia sugeridas.	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
ListTestRecommendations	Otorga permiso para enumerar recomendaciones de pruebas.	Enumeración	application*		
ListUnsupportedAppVersionResources	Otorga permiso para enumerar los recursos de versión de la aplicación no compatibles.	Enumeración	application*		
PublishAppVersion	Otorga permiso para publicar la versión de la aplicación.	Escritura	application*		
PutDraftAppVersionTemplate	Otorga permiso para colocar una plantilla de versión de borrador de la aplicación.	Escritura	application*		
RejectResourceGroupingRecommendations	Concede permiso para rechazar recomendaciones de agrupamiento de recursos	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RemoveDraftAppVersionResourceMappings	Otorga permiso para eliminar asignaciones de versión de borrador de la aplicación.	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResolveAppVersionResources	Otorga permiso para resolver recursos de versión de la aplicación.	Escritura	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartAppAssessment	Otorga permiso para crear una evaluación de aplicación.	Escritura	application*		cloudformation:DescribeStacks cloudformation:ListStackResources cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:GetMetricStatistics cloudwatch:PutMetricData ec2:DescribeRegions fis:GetExperimentTemplate

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					fis:ListExperimentTemplates fis:ListExperiments resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources ssm:GetParametersByPath

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
StartMetricsExport	Otorga permiso para iniciar la exportación de métricas	Escritura			
StartResourceGroupingRecommendationTask	Concede permiso para iniciar el proceso de generación de recomendaciones de agrupamiento de recursos	Escritura	application*		
TagResource	Concede permiso para asignar una etiqueta de recurso.	Etiquetado	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		
				aws:TagKeys	
UpdateApp	Otorga permiso para actualizar una aplicación.	Escritura	application*		iam:PassRole
UpdateAppVersion	Otorga permiso para actualizar una versión de aplicación	Escritura	application*		
UpdateAppVersionAppComponent	Otorga permiso para actualizar un componente de aplicación	Escritura	application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAppVersionResource	Otorga permiso para actualizar un recurso de aplicación	Escritura	application*		
UpdateResiliencyPolicy	Otorga permiso para actualizar una política de resiliencia.	Escritura	resiliency-policy*		

Tipos de recurso definidos por AWS Resilience Hub

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
resiliency-policy	`arn:${Partition}:resiliencehub:${Region}:${Account}:resiliency-policy/${ResiliencyPolicyId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:resiliencehub:${Region}:${Account}:app/${AppId}`	aws:ResourceTag/${TagKey}
app-assessment	`arn:${Partition}:resiliencehub:${Region}:${Account}:app-assessment/${AppAssessmentId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
recommendation-template	`arn:${Partition}:resiliencehub:${Region}:${Account}:recommendation-template/${RecommendationTemplateId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Resilience Hub

AWS Resilience Hub define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Administrador de acceso a recursos de AWS (RAM)

AWS Resource Access Manager (RAM) (prefijo de servicio:`ram`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Administrador de acceso a recursos de AWS (RAM)
- Tipos de recursos definidos por Administrador de acceso a recursos de AWS (RAM)
- Claves de condición para Administrador de acceso a recursos de AWS (RAM)

Acciones definidas por Administrador de acceso a recursos de AWS (RAM)

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de

recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptResourceShareInvitation	Otorga permiso para aceptar la invitación de recurso compartido especificado	Escritura	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateResourceShare	Otorga permiso para asociar los recursos and/or principales a un recurso compartido	Escritura	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	Otorga permiso para asociar un permiso a un recurso compartido	Escritura	customer-managed-permission*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			permission*		
			resource-share*		
CreatePermission	Otorga permiso para crear un permiso que se puede asociar a un recurso compartido	Escritura		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	Otorga permiso para crear una nueva versión de un permiso que se puede asociar a un recurso compartido	Escritura	customer-managed-permission*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ram:PermissionArn ram:PermissionResourceType	
CreateResourceShare	Otorga permiso para crear un recurso compartido con los and/or principales recursos proporcionados	Escritura		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeletePermission	Otorga permiso para eliminar un permiso específico	Escritura	customer-managed-permission*		
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	Otorga permiso para eliminar una versión específica de un permiso	Escritura	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	Otorga permiso para eliminar un recurso compartido	Escritura	resource-share*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
DisassociateResourceShare	Otorga permiso para desasociar los recursos and/or principales de un recurso compartido	Escritura	resource-share*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
DisassociateResourceSharePermission	Otorga permiso para desasociar un permiso de un recurso compartido	Write	customer-managed-permission* – permission*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			resource-share*		
EnableSharingWithAwsOrganization	Otorga permiso para obtener acceso a la organización del cliente y crear un SLR en la cuenta del cliente.	Administración de permisos			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	Otorga permiso para obtener el contenido de un permiso de AWS RAM	Lectura	customer-managed-permission*		
			permission*		
				ram:PermissionArn	
GetResourcePolicies	Otorga permiso para obtener las políticas de los recursos especificados que posee y que ha compartido	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourceShareAssociations	Otorga un permiso para obtener un conjunto de asociaciones de recursos compartidos de una lista proporcionada o con un estado específico del tipo especificado	Read			
GetResourceShareInvitations	Otorga permiso para obtener invitaciones de uso compartido de recursos mediante el ARN de invitación especificado o aquellos del recurso compartido	Read			
GetResourceShares	Otorga permiso para obtener un conjunto de recursos compartidos de una lista proporcionada o con un estado especificado	Read		aws:RequestTag/${TagKey} aws:TagKeys	
ListPendingInvitationResources	Otorga permiso para enumerar los recursos de un recurso compartido que se comparte con usted, pero que tiene la invitación todavía pendiente	Lectura	resource-share-invitation*		
				ram:ResourceShareName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPermissionAssociations	Concede permiso para enumerar información sobre el permiso y cualquier asociación	Enumeración	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	Otorga permiso para enumerar las versiones de un permiso de AWS RAM	Enumeración			
ListPermissions	Otorga permiso para enumerar los permisos de AWS RAM	Enumeración			
ListPrincipals	Otorga permiso para enumerar las entidades principales con las que ha compartido recursos o que tienen recursos compartidos con usted	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListReplacePermissionAssociationsWork	Otorga permiso para recuperar el estado del reemplazo de permiso asíncrono	Enumeración			
ListResourceShareePermissions	Otorga permiso para enumerar los permisos asociados a un recurso compartido	Enumeración	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
ListResourceTypes	Otorga permiso para enumerar los tipos de recursos que se pueden compartir y que admite la RAM AWS	Enumeración			
ListResources	Otorga permiso para enumerar los recursos que agregó a recursos compartidos o los recursos que se comparten con usted	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PromotePermissionCreatedFromPolicy	Otorga permiso para crear un permiso independiente y totalmente administrable por el cliente	Escritura	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
PromoteResourceShareCreatedFromPolicy	Otorga permiso para promover el recurso compartido especificado	Write	resource-share*		
RejectResourceShareInvitation	Otorga permiso para rechazar la invitación de recurso compartido especificada	Escritura	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ReplacePermissionAssociations	Concede permiso para actualizar todos los recursos compartidos a un nuevo permiso	Escritura	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
SetDefaultPermissionVersion	Otorga permiso para especificar un número de versión como versión predeterminada para el permiso administrado por el cliente correspondiente	Escritura	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
TagResource	Otorga permiso para etiquetar el recurso compartido especificado o el permiso	Etiquetado	customer-managed-permission		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar las etiquetas del recurso compartido especificado o del permiso	Etiquetado	customer-managed-permission		
			resource-share		
				aws:TagKeys	
UpdateResourceShare	Otorga permiso para actualizar atributos del recurso compartido	Escritura	resource-share*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals	

Tipos de recursos definidos por Administrador de acceso a recursos de AWS (RAM)

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
resource-share	arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}	aws:ResourceTag/${TagKey} ram:AllowsExternalPrincipals ram:ResourceShareName
resource-share-invitation	arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}	ram:ShareOwnerAccountId
permission	arn:${Partition}:ram::${Account}:permission/${ResourcePath}	ram:PermissionArn ram:PermissionResourceType
customer-managed-permission	arn:${Partition}:ram:${Region}:${Account}:permission/${ResourcePath}	aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType

Claves de condición para Administrador de acceso a recursos de AWS (RAM)

AWS Resource Access Manager (RAM) define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso en función de las etiquetas que se pasan en la solicitud al crear o etiquetar un recurso compartido Si los usuarios no transmiten estas etiquetas en concreto o si no especifican ninguna etiqueta, la solicitud dará un error.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de las claves de etiqueta que se pasan al crear o etiquetar un recurso compartido	ArrayOfString
ram:AllowsExternalPrincipals	Filtra el acceso en función de los recursos compartidos que permiten o deniegan el uso compartido con entidades principales externas. Por ejemplo, especifica true si la acción solo se puede realizar en recursos compartidos de recursos que permiten el uso compartido con entidades principales externas. Los principales externos son AWS cuentas que están fuera de su organización AWS	Bool
ram:PermissionArn	Filtra el acceso en función del ARN de permiso especificado	ARN
ram:PermissionResourceType	Filtra el acceso en función de los permisos del tipo de recurso especificado	Cadena
ram:Principal	Filtra el acceso en función del formato de la entidad principal especificada	Cadena
ram:RequestedAllow	Filtra el acceso según el valor especificado para 'allowExternalPrincipals'. Los directores externos son AWS	Bool

Claves de condición	Descripción	Tipo
sExternal Principals	cuentas que se encuentran fuera de su organización AWS	
ram:Reque stedResou rceType	Filtra el acceso en función del tipo de recurso especific ado	Cadena
ram:Resou rceArn	Filtra el acceso en función del ARN especificado	ARN
ram:Resou rceShareName	Filtra el acceso en función de un recurso compartido con el nombre especificado	Cadena
ram:Resou rceTag/${ TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
ram:Share OwnerAccountId	Filtra el acceso en función de los recursos compartid os propiedad de una cuenta específica. Por ejemplo, puede utilizar esta clave de condición para especific ar qué invitaciones de uso compartido de recursos se pueden aceptar o rechazar en función del ID de cuenta del propietario del recurso compartido	Cadena

Acciones, recursos y claves de condición para AWS Resource Explorer

AWS El explorador de recursos (prefijo de servicio:`resource-explorer-2`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Resource Explorer
- Tipos de recursos definidos por AWS Resource Explorer
- Claves de condición para AWS Resource Explorer

Acciones definidas por AWS Resource Explorer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateDefaultView	Otorga permiso para establecer la vista especificada como predeterminada para esto Región de AWS en este Cuenta de AWS	Escritura			
BatchGetView	Otorga permiso para recuperar detalles sobre las vistas que especifique mediante una lista de ARNs	Lectura			resource-explorer-2:GetView
CreateIndex	Concede permiso para activar el Explorador de recursos Región de AWS en el que se realizó esta operación mediante la creación de un índice	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedView	Otorga permiso para crear una vista administrada	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
[solo permiso]					
CreateView	Otorga permiso para crear una vista que los usuarios puedan consultar	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIndex	Otorga permiso para desactivar el Explorador de recursos en la zona especificada Región de AWS mediante la eliminación del índice	Escritura	index*		
DeleteResourcePolicy [solo permiso]	Concede permiso para eliminar la política de recursos de la vista especificada	Administración de permisos	view*		
DeleteView	Otorga permiso para eliminar una vista	Escritura	view*		
DisassociateDefaultView	Otorga permiso para eliminar la vista predeterminada de Región de AWS la que se llama a esta operación	Escritura			
GetAccountLevelServiceConfiguration	Otorga permiso a Resource Explorer para acceder a los datos a nivel de cuenta de su AWS organización	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDefaultView	Otorga permiso para recuperar el nombre de recurso de Amazon (ARN) de la vista que es el predeterminado para la operación Región de AWS en la que se llama a esta operación	Lectura			
GetIndex	Otorga permiso para recuperar información sobre el índice Región de AWS en el que se llama a esta operación	Lectura			
GetManagedView	Otorga permiso para obtener la vista gestionada	Lectura	managed-view*		
GetResourcePolicy [solo permiso]	Concede permiso para recuperar información sobre la política de recursos de la vista especificada	Lectura	view*		
GetView	Otorga permiso para devolver información acerca de la vista especificada	Lectura	view*		
ListIndexes	Otorga permiso para enumerar todos los índices Regiones de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIndexesForMembers	Otorga permiso para incluir todos los índices de las cuentas de los miembros de la organización Regiones de AWS	Enumeración			
ListManagedViews	Otorga permiso para enumerar las vistas administradas	Enumeración			
ListSupportedResourceTypes	Otorga permiso para recuperar una lista de todos los tipos de recursos actualmente compatibles con Resource Explorer	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas adjuntas al recurso especificado	Lectura	index view		
ListViews	Otorga permiso para enumerar los nombres de los recursos de Amazon (ARNs) de todas las vistas disponibles Región de AWS en las que se llama a esta operación	Enumeración			
PutResourcePolicy [solo permiso]	Concede permiso para actualizar la política de recursos de la vista especificada	Administración de permisos	view*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Search	Otorga permiso para buscar recursos y mostrar detalles sobre todos los recursos que coinciden con los criterios especificados	Lectura	view*		
				resource-explorer-2:Operation	
TagResource	Otorga permiso para agregar uno o más pares de clave-valor de etiqueta al recurso especificado	Etiquetado	index		
			view		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar uno o más pares de clave-valor de etiqueta al recurso especificado	Etiquetado	index		
			view		
				aws:TagKeys	
UpdateIndexType	Otorga permiso para cambiar el tipo de índice de LOCAL a AGGREGATOR o viceversa	Escritura	index*		
UpdateView	Otorga permiso para modificar algunos detalles de una vista	Escritura	view*		

Tipos de recursos definidos por AWS Resource Explorer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${ViewUuid}`	aws:ResourceTag/${TagKey}
index	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${IndexUuid}`	aws:ResourceTag/${TagKey}
managed-view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:managed-view/${ManagedViewName}/${ManagedViewUuid}`	

Claves de condición para AWS Resource Explorer

AWS El explorador de recursos define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las claves de etiqueta asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
resource-explorer-2:Operation	Filtra el acceso por la operación real que se está invocando, valores disponibles: Buscar, ListResources	Cadena

Claves de condición, recursos y acciones de la API de etiquetado de grupos de recursos de Amazon

La API de etiquetado de grupos de recursos de Amazon (prefijo de servicio: `tag`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la API de etiquetado de grupos de recursos de Amazon
- Tipos de recursos definidos por la API de etiquetado de grupos de recursos de Amazon
- Claves de condición de la API de etiquetado de grupos de recursos de Amazon

Acciones definidas por la API de etiquetado de grupos de recursos de Amazon

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeReportCreation	Otorga permiso para describir el estado de la operación StartReportCreation	Lectura			
GetComplianceSummary	Concede permiso para recuperar un resumen de la cantidad de recursos que no cumplen con las políticas de etiquetas efectivas	Lectura			
GetResources	Otorga permiso para devolver los recursos etiquetados o previamente etiquetados en la cuenta Región de AWS de llamada especificada	Lectura			
GetTagKeys	Otorga permiso para devolver las claves de etiquetas actualmente en uso en la cuenta especificada Región de AWS para la cuenta que realiza la llamada	Lectura			
GetTagValues	Otorga permiso para devolver los valores de etiqueta de la clave especificada que se utilizan en la cuenta especificada Región de AWS para la llamada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartReportCreation	Concede permiso para iniciar la generación de un informe que mencione todos los recursos etiquetados en las cuentas de la organización y si cada recurso cumple con la política de etiquetas efectiva	Escritura			
TagResources	Concede permiso para aplicar una o más etiquetas a los recursos especificados	Etiquetado			
UntagResources	Concede el permiso para quitar las etiquetas especificadas de los recursos especificados.	Etiquetado			

Tipos de recursos definidos por la API de etiquetado de grupos de recursos de Amazon

La API de etiquetado de grupos de recursos de Amazon no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a la API de etiquetado de grupos de recursos de Amazon, especifique `"Resource": "*"` en su política.

Claves de condición de la API de etiquetado de grupos de recursos de Amazon

El etiquetado de grupos de recursos no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Resource Groups

AWS Resource Groups (prefijo de servicio:`resource-groups`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Resource Groups
- Tipos de recursos definidos por AWS Resource Groups
- Claves de condición para AWS Resource Groups

Acciones definidas por AWS Resource Groups

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateResource [solo permiso]	Concede permiso para asociar un recurso con una aplicación	Escritura	group*		
CancelTagSyncTask	Concede permiso para cancelar una tarea de sincronización de etiquetas para un grupo de aplicaciones	Escritura	group*		resource-groups:DeleteGroup

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateGroup	Concede permiso para crear un grupo de recursos con un nombre, descripción y consulta de recursos especificados.	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	Concede permiso para eliminar un grupo de recursos especificados.	Escritura	group*		tag:GetResources
DeleteGroupPolicy [solo permiso]	Concede permiso para eliminar una política basada en recursos para el grupo especificado	Escritura	group*		
DisassociateResource [solo permiso]	Concede permiso para desasociar un recurso de una aplicación	Escritura	group*		
GetAccountSettings	Otorga permiso para obtener el estado actual de características opcionales en Resource Groups	Lectura			
GetGroup	Concede permiso para obtener información de un grupo de recursos especificado.	Read	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGroupConfiguration	Concede permiso para obtener la configuración del servicio asociada al grupo de recursos especificado.	Lectura	group*		
GetGroupPolicy [solo permiso]	Concede permiso para obtener una política basada en recursos para el grupo especificado	Lectura	group*		
GetGroupQuery	Concede permiso para obtener la consulta asociada a un grupo de recursos especificado.	Lectura	group*		
GetTagSyncTask	Concede permiso para obtener información de una tarea de sincronización de etiquetas especificada	Lectura	group*		
GetTags	Concede permiso para obtener las etiquetas asociadas a un grupo de recursos especificado.	Read	group*		
GroupResources	Concede permiso para agregar los recursos especificados al grupo especificado.	Write	group*		resource-groups:Tag tag:TagResources

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGroupResources	Concede permiso para enumerar los recursos que son miembros de un grupo de recursos especificado.	Enumeración	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	Concede permiso para enumerar los estados de agrupación de un grupo de aplicaciones especificado	Enumeración	group*		
ListGroups	Concede permiso para enumerar todos los grupos de recursos de su cuenta.	Enumeración			
ListResourceTypes [solo permiso]	Concede permiso para enumerar los tipos de recursos admitidos	Enumeración			
ListTagSyncTasks	Concede permiso para enumerar todas las tareas de sincronización de etiquetas en la cuenta	Enumeración	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutGroupConfiguration	Concede permiso para poner la configuración del servicio asociada al grupo de recursos especificado	Write	group*		
PutGroupPolicy [solo permiso]	Concede permiso para agregar una política basada en los recursos para el grupo especificado.	Escritura	group*		
SearchResources	Otorga permiso para buscar AWS recursos que coincidan con la consulta dada	Enumeración			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
StartTagSyncTask	Concede permiso para crear una tarea de sincronización de etiquetas para un grupo de aplicaciones	Escritura	group*		iam:PassRole resource-groups:CreateGroup
Tag	Concede permiso para etiquetar un grupo de recursos especificado.	Etiquetado	group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UngroupResources	Concede permiso para quitar los recursos especificados del grupo especificado.	Write	group*		resource-groups:Untag tag:UntagResources
Untag	Concede permiso para quitar las etiquetas asociadas a un grupo de recursos especificado.	Etiquetado	group*		
				aws:TagKeys	
UpdateAccountSettings	Otorga permiso para actualizar características opcionales en Resource Groups	Escritura			
UpdateGroup	Concede permiso para actualizar un grupo de recursos especificado.	Write	group*		
UpdateGroupQuery	Concede permiso para actualizar la consulta asociada a un grupo de recursos especificado.	Write	group*		cloudformation:DescribeStacks

Tipos de recursos definidos por AWS Resource Groups

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
group	`arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}`	aws:ResourceTag/${TagKey}
tagSyncTask	`arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}/tag-sync-task/${TaskId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Resource Groups

AWS Resource Groups define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon RHEL Knowledgebase Portal

Amazon RHEL Knowledgebase Portal (prefijo de servicio: `rhelkb`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon RHEL Knowledgebase Portal
- Tipos de recursos definidos por Amazon RHEL Knowledgebase Portal
- Claves de condición para Amazon RHEL Knowledgebase Portal

Acciones definidas por Amazon RHEL Knowledgebase Portal

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRhelURL	Concede permiso para acceder al portal Red Hat Knowledgebase	Lectura			

Tipos de recursos definidos por Amazon RHEL Knowledgebase Portal

Amazon RHEL Knowledgebase Portal no permite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Amazon RHEL Knowledgebase Portal, especifique `"Resource": "*"` en su política.

Claves de condición para Amazon RHEL Knowledgebase Portal

RHEL KB no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS RoboMaker

AWS RoboMaker (prefijo de servicio:`robomaker`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS RoboMaker

- Tipos de recursos definidos por AWS RoboMaker
- Claves de condición de AWS RoboMaker

Acciones definidas por AWS RoboMaker

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDeleteWorlds	Eliminar uno o más mundos en una operación por lotes	Write			
BatchDescribeSimulationJob	Describir varios trabajos de simulación	Read			
CancelDeploymentJob	Cancelar un trabajo de implementación	Write	deploymentJob*		
CancelSimulationJob	Para cancelar un trabajo de simulación	Write	simulationJob*		
CancelSimulationJobBatch	Cancela un lote de trabajos de simulación	Write	simulationJobBatch*		
CancelWorldExportJob	Cancelar un trabajo de exportación de mundo	Write	worldExportJob*		
CancelWorldGenerationJob	Cancelar un trabajo de generación de mundos	Write	worldGenerationJob*		
CreateDeploymentJob	Creación de un trabajo de implementación	Write		aws:TagKeys	iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	
CreateFleet	Crear una flota de implementación que representa un grupo lógico de robots que ejecutan la misma aplicación de robots	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobot	Crear un robot que puede registrarse en una flota	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateRobotApplication	Crear una aplicación de robot	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobotApplicationVersion	Crear una instantánea de una aplicación de robot	Write	robotApplication*		s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSimulationApplication	Crear una aplicación de simulación	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSimulationApplicationVersion	Crear una instantánea de una aplicación de simulación	Write	simulationApplication*		s3:GetObject
CreateSimulationJob	Crear un trabajo de simulación	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateWorldExportJob	Crear un trabajo de exportación de mundo	Write	world*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldGenerationJob	Crear un trabajo de generación de mundo	Write	worldTemplate*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldTemplate	Crear una plantilla de mundo	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteFleet	Eliminación de un grupo de implementaciones	Write	deploymentFleet*		
DeleteRobot	Para eliminar un robot	Write	robot*		
DeleteRobotApplication	Para eliminar una aplicación de robot	Write	robotApplication*		
DeleteSimulationApplication	Para eliminar una aplicación de simulación	Write	simulationApplication*		
DeleteWorldTemplate	Eliminar una plantilla de mundo	Write	worldTemplate*		
DeregisterRobot	Anular el registro de un robot de una flota	Write	deploymentFleet* robot*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDeploymentJob	Describir una tarea de implementación	Read	deploymentJob*		
DescribeFleet	Describir una flota de implementación	Read	deploymentFleet*		
DescribeRobot	Describir un robot	Read	robot*		
DescribeRobotApplication	Describir una aplicación de robot	Read	robotApplication*		
DescribeSimulationApplication	Crear una aplicación de simulación	Read	simulationApplication*		
DescribeSimulationJob	Describir un trabajo de simulación	Read	simulationJob*		
DescribeSimulationJobBatch	Describe un lote de trabajos de simulación	Read	simulationJobBatch*		
DescribeWorld	Describir un mundo	Read	world*		
DescribeWorldExportJob	Describir un trabajo de exportación de mundo	Read	worldExportJob*		
DescribeWorldGenerationJob	Describir un trabajo de generación de mundos	Read	worldGenerationJob*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeWorldTemplate	Describir una plantilla de mundo	Read	worldTemplate*		
GetWorldTemplateBody	Obtener el cuerpo de una plantilla de mundo	Read	worldTemplate*		
ListDeploymentJobs	Generar una lista de los trabajos de implementación	List			
ListFleets	Generar una lista de las flotas	List			
ListRobotApplications	Generar una lista de aplicaciones de robot	List			
ListRobots	Generar una lista de robots	List			
ListSimulationApplications	Generar una lista de las aplicaciones de simulación	List			
ListSimulationJobBatches	Muestra los lotes de trabajos de simulación	List			
ListSimulationJobs	Generar una lista de los trabajos de simulación	List			
ListSupportedAvailabilityZones [solo permiso]	Enumera las zonas de disponibilidad admitidas	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Enumere las etiquetas de un recurso RoboMaker	Enumeración	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
ListWorldExportJobs	Enumerar trabajos de exportación de mundo	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWorldGenerationJobs	Enumerar trabajos de generación de mundos	List			
ListWorldTemplates	Enumerar plantillas de mundo	List			
ListWorlds	Enumerar mundos	List			
RegisterRobot	Registrar un robot en una flota	Write	deploymentFleet*		
			robot*		
RestartSimulationJob	Reiniciar un trabajo de simulación en ejecución	Write	simulationJob*		
StartSimulationJobBatch	Crea un lote de trabajos de simulación	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
SyncDeploymentJob	Garantiza que se haya implementado la última aplicación de robots implementada a todos los robots de la flota	Escritura	deploymentFleet*		iam:CreateServiceLinkedRole
TagResource	Añadir etiquetas a un RoboMaker recurso	Etiquetado	deploymentFleet		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Eliminar etiquetas de un RoboMaker recurso	Etiquetado	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys	
UpdateRobotApplication	Actualizar una aplicación de robot	Write	robotApplication*		
UpdateRobotDeployment [solo permiso]	Informar sobre el estado de implementación de un robot individual	Write			
UpdateSimulationApplication	Actualizar una aplicación de simulación	Write	simulationApplication*		
UpdateWorldTemplate	Actualizar una plantilla de mundo	Escritura	worldTemplate*		

Tipos de recursos definidos por AWS RoboMaker

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
robotApplication	arn:${Partition}:robomaker:${Region}:${Account}:robot-application/${ApplicationName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
simulationApplication	arn:${Partition}:robomaker:${Region}:${Account}:simulation-application/${ApplicationName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
simulationJob	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job/${SimulationJobId}	aws:ResourceTag/${TagKey}
simulationJobBatch	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job-batch/${SimulationJobBatchId}	aws:ResourceTag/${TagKey}
deploymentJob	arn:${Partition}:robomaker:${Region}:${Account}:deployment-job/${DeploymentJobId}	aws:ResourceTag/${TagKey}
robot	arn:${Partition}:robomaker:${Region}:${Account}:robot/${RobotName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
deploymentFleet	arn:${Partition}:robomaker:${Region}:${Account}:deployment-fleet/${FleetName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
worldGenerationJob	arn:${Partition}:robomaker:${Region}:${Account}:world-generation-job/${WorldGenerationJobId}	aws:ResourceTag/${TagKey}
worldExportJob	arn:${Partition}:robomaker:${Region}:${Account}:world-export-job/${WorldExportJobId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
worldTemplate	`arn:${Partition}:robomaker:${Region}:${Account}:world-template/${WorldTemplateJobId}`	aws:ResourceTag/${TagKey}
world	`arn:${Partition}:robomaker:${Region}:${Account}:world/${WorldId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS RoboMaker

AWS RoboMaker define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Route 53

Amazon Route 53 (prefijo de servicio: `route53`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Route 53
- Tipos de recurso definidos por Amazon Route 53
- Claves de condición de Amazon Route 53

Acciones definidas por Amazon Route 53

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateKeySigningKey	Concede permiso para activar una clave de firma de clave para que las DNSSEC puedan usarla para firmar	Write	hostedzone*		
AssociateVPCWithHostedZone	Concede permiso para asociar un Amazon VPC adicional con una zona hospedada privada.	Escritura	hostedzone		ec2:DescribeVpcs
				route53:VPCs	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ChangeCidrCollection	Otorga permiso para crear o eliminar bloques de CIDR dentro de una colección CIDR	Escritura	cidrcollection*		
ChangeResourceRecordSets	Concede permiso para crear, actualizar o eliminar un registro, que contiene información de DNS de autorización para un nombre de dominio o subdominio especificados.	Write	hostedzone*		
				route53:ChangeResourceRecordSetsNormalizedRecordNames route53:ChangeResourceRecordSetsRecordTypes route53:ChangeResourceRecordSetsActions	
ChangeTagsForResource	Otorga permiso para agregar, editar o eliminar etiquetas para una comprobación de estado o una zona alojada.	Etiquetado	healthcheck*		
			hostedzone*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCidrCollection	Otorga permiso para crear una nueva colección CIDR	Escritura			
CreateHealthCheck	Concede permiso para crear una nueva comprobación de estado que monitorea el estado y el desempeño de sus aplicaciones web, servidores web y otros recursos.	Write			
CreateHostedZone	Concede permiso para crear una zona hospedada pública, que se utiliza para especificar la manera en que el sistema de nombres de dominio (DNS) redirige el tráfico en Internet para un dominio (como example.com) y sus subdominios.	Write		route53:VPCs	ec2:DescribeVpcs
CreateKeySigningKey	Concede permiso para crear una nueva clave de firma de clave asociada a una zona alojada	Write	hostedzone*		
CreateQueryLoggingConfig	Concede permiso para crear una configuración para el registro de consultas de DNS.	Write	hostedzone*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateReusableDelegationSet	Concede permiso para crear un conjunto de delegación (un grupo de cuatro servidores de nombres) que pueden reutilizar varias zonas hospedadas.	Write			
CreateTrafficPolicy	Otorga permiso para crear una política de tráfico, que se utiliza para crear varios registros de DNS de un nombre de dominio (como example.com) o un nombre de subdominio (como www.example.com).	Write			
CreateTrafficPolicyInstance	Concede permiso para crear los registros de una zona hospedada especificada en función de la configuración de una determinada versión de política de tráfico.	Write	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	Concede permiso para crear una nueva versión de una política de tráfico existente.	Escritura	trafficpolicy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateVPCAssociationAuthorization	Otorga permiso para autorizar a la persona Cuenta de AWS que creó una VPC específica a enviar una VPCWithHostedZone solicitud de asociado, que asocia la VPC a una zona alojada específica que fue creada por una cuenta diferente	Escritura	hostedzone*		
				route53:VPCs	
DeactivateKeySigningKey	Concede permiso para desactivar una clave de firma de clave para que las DNSSEC no la usen para firmar	Escritura	hostedzone*		
DeleteCidrCollection	Otorga permiso para eliminar una colección CIDR	Escritura	cidrcollection*		
DeleteHealthCheck	Concede permiso para eliminar una comprobación de estado.	Write	healthcheck*		
DeleteHostedZone	Concede permiso para eliminar una zona hospedada.	Write	hostedzone*		
DeleteKeySigningKey	Concede permiso para eliminar una clave de firma de clave	Write	hostedzone*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteQueryLoggingConfig	Concede permiso para eliminar una configuración para el registro de consultas de DNS.	Write	queryloggingconfig*		
DeleteReusableDelegationSet	Concede permiso para eliminar un conjunto de delegación reutilizable.	Write	delegationset*		
DeleteTrafficPolicy	Concede permiso para eliminar una política de tráfico.	Write	trafficpolicy*		
DeleteTrafficPolicyInstance	Concede permiso para eliminar una instancia de política de tráfico y todos los registros que Route 53 creó cuando usted creó la instancia .	Write	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Concede permiso para quitar la autorización asociar una Amazon Virtual Private Cloud con una zona hospedada privada Route 53.	Write	hostedzone*		
				route53:VPCs	
DisableHostedZoneDNSSEC	Otorga permiso para desactivar la firma de DNSSEC en una zona alojada específica	Write	hostedzone*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateVPCFromHostedZone	Concede permiso para desasociar una Amazon Virtual Private Cloud de una zona hospedada privada Route 53.	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
EnableHostedZoneDNSSEC	Concede permiso para habilitar la firma de DNSSEC en una zona alojada específica	Write	hostedzone*		
GetAccountLimit	Concede permiso para obtener el límite especificado para la cuenta actual, por ejemplo, el número máximo de comprobaciones de estado que puede crear con la cuenta.	Read			
GetChange	Concede permiso para obtener el estado actual de una solicitud para crear, actualizar o eliminar uno o varios registros.	List	change*		
GetCheckerIpRanges	Concede permiso para obtener una lista de los rangos de IP que utilizan los comprobadores de estado de Route 53 para comprobar el estado de los recursos.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDNSSEC	Concede permiso para obtener información sobre DNSSEC para una zona alojada específica, incluidas las claves de firma de claves en la zona alojada	Read	hostedzone*		
GetGeoLocation	Concede permiso para obtener información acerca de si una ubicación geográfica especificada es compatible con los registros de geolocalización Route 53.	List			
GetHealthCheck	Concede permiso para obtener información acerca de una comprobación de estado especificada.	Lectura	healthcheck*		
GetHealthCheckCount	Otorga permiso para obtener el número de comprobaciones de estado asociadas a la actual Cuenta de AWS	Enumeración			
GetHealthCheckLastFailureReason	Concede permiso para obtener la razón por la que una comprobación de estado especificada fue errónea más recientemente.	List	healthcheck*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetHealthCheckStatus	Concede permiso para obtener el estado de una comprobación de estado especificada.	List	healthcheck*		
GetHostedZone	Concede permiso para obtener información acerca de una zona hospedada especificada, incluidos los cuatro servidores de nombres que Route 53 asignó a la zona hospedada.	Enumeración	hostedzone*		
GetHostedZoneCount	Otorga permiso para obtener el número de zonas alojadas asociadas a la actual Cuenta de AWS	Enumeración			
GetHostedZoneLimit	Concede permiso para obtener el límite especificado para una zona hospedada especificada.	Read	hostedzone*		
GetQueryLoggingConfig	Concede permiso para obtener información acerca de una configuración especificada para el registro de consultas de DNS.	Read	queryloggingconfig*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetReusableDelegationSet	Concede permiso para obtener información acerca de un conjunto de delegación reutilizable especificado, incluidos los cuatro servidores de nombres que están asignados al conjunto de delegación.	List	delegationset*		
GetReusableDelegationSetLimit	Concede permiso para obtener el número máximo de zonas hospedadas que puede asociar al conjunto de delegación reutilizable especificado.	Read	delegationset*		
GetTrafficPolicy	Concede permiso para obtener información acerca de una versión de política de tráfico especificada.	Read	trafficpolicy*		
GetTrafficPolicyInstance	Concede permiso para obtener información acerca de una instancia de política de tráfico especificada.	Lectura	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	Otorga permiso para obtener el número de instancias de política de tráfico asociadas a la actual Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCidrBlocks	Otorga permiso para obtener una lista de los bloques CIDR dentro de una colección CIDR especificada	Enumeración	cidrcollection*		
ListCidrCollections	Otorga permiso para obtener una lista de las colecciones del CIDR asociadas a la actual Cuenta de AWS	Enumeración			
ListCidrLocations	Otorga permiso para obtener una lista de ubicaciones CIDR que pertenecen a una colección CIDR especificada	Enumeración	cidrcollection*		
ListGeoLocations	Concede permiso para obtener una lista de ubicaciones geográficas que Route 53 admite para geolocalización.	Lectura			
ListHealthChecks	Otorga permiso para obtener una lista de los controles de estado asociados a la actual Cuenta de AWS	Lectura			
ListHostedZones	Otorga permiso para obtener una lista de las zonas alojadas públicas y privadas asociadas a la actual Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListHostedZonesByName	Concede permiso para obtener una lista de sus zonas hospedadas en orden lexicográfico. Las zonas alojadas se ordenan por nombre con las etiquetas invertidas; por ejemplo, com.example.www	Enumeración			
ListHostedZonesByVPC	Concede permiso para obtener una lista de todas las zonas alojadas privadas con las que está asociada una VPC especificada	Enumeración		route53:VPCs	ec2:DescribeVpcs
ListQueryLoggingConfigs	Otorga permiso para enumerar las configuraciones del registro de consultas de DNS asociadas a la zona alojada actual Cuenta de AWS o a la configuración asociada a una zona alojada específica	Enumeración	hostedzone		
ListResourceRecordSets	Concede permiso para enumerar los registros de una zona hospedada especificada.	Enumeración	hostedzone*		
ListReusableDelegationSets	Otorga permiso para enumerar los conjuntos de delegación reutilizables asociados con la Cuenta de AWS actual.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas de una comprobación de estado o zona hospedada	Lectura	healthcheck		
			hostedzone		
ListTagsForResources	Concede permiso para enumerar las etiquetas de hasta 10 comprobaciones de estado o zonas hospedadas.	Lectura	healthcheck		
			hostedzone		
ListTrafficPolicies	Otorga permiso para obtener información acerca de la versión más reciente de cada política de tráfico asociada a la Cuenta de AWS actual. Las políticas están enumeradas en el orden en el que se crearon	Enumeración			
ListTrafficPolicyInstances	Otorga permiso para obtener información sobre las instancias de política de tráfico que ha creado con la actual Cuenta de AWS	Lectura			
ListTrafficPolicyInstancesByHostedZone	Concede permiso para obtener información acerca de las instancias de políticas de tráfico que haya creado en una zona hospedada especificada.	List	hostedzone*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTrafficPolicyInstancesByPolicy	Concede permiso para obtener información acerca de las instancias de políticas de tráfico que haya creado usando una versión de política de tráfico especificada.	List	trafficpolicy*		
ListTrafficPolicyVersions	Concede permiso para obtener información acerca de todas las versiones de una política de tráfico especificada.	Enumeración	trafficpolicy*		
ListVPCAssociationAuthorizations	Otorga permiso para obtener una lista de las VPCs que han creado otras cuentas y que se pueden asociar a una zona alojada específica	Enumeración	hostedzone*		
TestDNSAnswer	Concede permiso para obtener el valor que Route 53 devuelve en respuesta a una consulta de DNS para un nombre de registro y tipo especificados.	Read			
UpdateHealthCheck	Concede permiso para actualizar una comprobación de estado existente.	Write	healthcheck*		
UpdateHostedZoneComment	Concede permiso para actualizar el comentario de una zona hospedada especificada.	Write	hostedzone*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTrafficPolicyComment	Concede permiso para actualizar el comentario de una versión de política de tráfico especificada.	Write	trafficpolicy*		
UpdateTrafficPolicyInstance	Concede permiso para actualizar los registros de una zona hospedada especificada que se crearon basados en la configuración de una determinada versión de política de tráfico.	Write	trafficpolicyinstance*		

Tipos de recurso definidos por Amazon Route 53

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cidrcollection	`arn:${Partition}:route53:::cidrcollection/${Id}`	
change	`arn:${Partition}:route53:::change/${Id}`	

Tipos de recurso	ARN	Claves de condición
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}	

Claves de condición de Amazon Route 53

Amazon Route 53 define las siguientes claves de condiciones que se pueden usar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
route53:ChangeResourceRecordSetsActions	Filtra el acceso mediante las acciones de cambio CREATE, UPSERT o DELETE de una solicitud ChangeResourceRecordSets	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	Filtra el acceso por los nombres de los registros DNS normalizados de una solicitud ChangeResourceRecordSets	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	Filtra el acceso por los tipos de registros DNS de una solicitud ChangeResourceRecordSets	ArrayOfString
route53:VPCs	Filtra el acceso VPCs por solicitud	Cadena

Acciones, recursos y claves de condición para Amazon Route 53 Domains

Amazon Route 53 Domains (prefijo de servicio: `route53domains`) ofrece los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Route 53 Domains
- Tipos de recurso definidos por los dominios de Amazon Route 53
- Claves de condición de Amazon Route 53 Domains

Acciones definidas por Amazon Route 53 Domains

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptDomainTransferFromAnotherAwsAccount	Otorga permiso para aceptar la transferencia de un dominio de otro Cuenta de AWS al actual Cuenta de AWS	Escritura			
AssociateDelegationSignerToDomain	Concede permiso para asociar un nuevo firmante de delegación a un dominio	Escritura			
CancelDomainTransferToAnotherAwsAccount	Otorga permiso para cancelar la transferencia de un dominio del dominio actual Cuenta de AWS a otro Cuenta de AWS	Escritura			
CheckDomainAvailability	Concede permiso para comprobar la disponibilidad de un nombre de dominio.	Read			
CheckDomainTransferability	Concede permiso para comprobar si un nombre de dominio puede transferirse a Amazon Route 53	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDomain	Otorga permiso para eliminar dominios	Escritura			
DeleteTagsForDomain	Concede permiso para eliminar las etiquetas especificadas de un dominio.	Etiquetado			
DisableDomainAutoRenew	Concede permiso para configurar Amazon Route 53 para que renueve automáticamente el dominio especificado antes de que caduque el registro del dominio.	Escritura			
DisableDomainTransferLock	Otorga permiso para eliminar el bloqueo de transferencia del dominio (específicamente el clientTransferProhibited estado) para permitir las transferencias de dominio	Escritura			
DisassociateDelegationSignerFromDomain	Concede permiso para desasociar un firmante de delegación existente de un dominio	Escritura			
EnableDomainAutoRenew	Concede permiso para configurar Amazon Route 53 para que renueve automáticamente el dominio especificado antes de que caduque el registro del dominio.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableDomainTransferLock	Otorga permiso para establecer el bloqueo de transferencia en el dominio (específicamente el clientTransferProhibited estado) a fin de impedir las transferencias de dominio	Escritura			
GetContactReachabilityStatus	Otorga permiso para obtener información sobre si el contacto solicitante ha respondido a las operaciones que requieren confirmar que la dirección de correo electrónico del titular es válida, por ejemplo, registrar un nuevo dominio	Lectura			
GetDomainDetail	Concede permiso para obtener información detallada acerca de un dominio.	Read			
GetDomainSuggestions	Concede permiso para devolver una lista de nombres de dominio sugeridos dada una cadena, que puede ser un nombre de dominio o simplemente una palabra o frase (sin espacios).	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOperationDetail	Concede permiso para obtener el estado actual de una operación que no se completó.	Lectura			
ListDomains	Otorga permiso para enumerar todos los nombres de dominio registrados en Amazon Route 53 para el actual Cuenta de AWS	Enumeración			
ListOperations	Otorga permiso para enumerar el funcionamiento IDs de las operaciones que aún no se han completado	Enumeración			
ListPrices	Otorga permiso para publicar los precios de las operaciones de TLDs	Enumeración			
ListTagsForDomain	Concede permiso para obtener una lista de todas las etiquetas que están asociadas con el dominio especificado.	Lectura			
PushDomain	Concede permiso para cambiar la etiqueta IPS del dominio .uk para iniciar un proceso de transferencia de Route 53 a otro registrador	Escritura			
RegisterDomain	Concede permiso para registrar dominios.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RejectDomainTransferFromAnotherAwsAccount	Otorga permiso para rechazar la transferencia de un dominio de otro Cuenta de AWS al actual Cuenta de AWS	Escritura			
RenewDomain	Concede permiso para renovar dominios para el número especificado de años.	Escritura			
ResendContactReachabilityEmail	Otorga permiso para reenviar el correo de confirmación a la dirección de correo electrónico para el contacto solicitante en las operaciones que requieren confirmar que la dirección de correo electrónico del titular es válida, por ejemplo, registrar un nuevo dominio	Escritura			
ResendOperationAuthorization	Concede permiso para volver a enviar la autorización de la operación	Escritura			
RetrieveDomainAuthCode	Otorga permiso AuthCode para obtener el nombre del dominio	Escritura			
TransferDomain	Concede permiso para transferir un dominio de otro registrador a Amazon Route 53.	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TransferDomainToAnotherAwsAccount	Otorga permiso para transferir un dominio del dominio actual Cuenta de AWS a otro Cuenta de AWS	Escritura			
UpdateDomainContact	Concede permiso para actualizar la información de contacto para un dominio.	Write			
UpdateDomainContactPrivacy	Concede permiso para actualizar la configuración de privacidad de contacto del dominio.	Write			
UpdateDomainNameservers	Concede permiso para sustituir el conjunto actual de servidores de nombres de un dominio por el conjunto de servidores de nombres especificado.	Write			
UpdateTagsForDomain	Otorga permiso para agregar o actualizar etiquetas para un dominio especificado.	Etiquetado			
ViewBilling	Otorga permiso para obtener todos los registros de facturación relacionados con el dominio del dominio actual Cuenta de AWS durante un período específico	Lectura			

Tipos de recurso definidos por los dominios de Amazon Route 53

Amazon Route 53 Domains no admite la especificación de un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso a Amazon Route 53 Domains, especifique `"Resource": "*"` en su política.

Claves de condición de Amazon Route 53 Domains

Route 53 Domains no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para los Perfiles de Amazon Route 53

Perfiles de Amazon Route 53 (prefijo del servicio: `route53profiles`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Perfiles de Amazon Route 53
- Tipos de recursos definidos por Perfiles de Amazon Route 53
- Claves de condición para Perfiles de Amazon Route 53

Acciones definidas por Perfiles de Amazon Route 53

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateProfile	Concede permiso para asociar un perfil a la VPC del cliente	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeVpcs
AssociateResourceToProfile	Concede permiso para asociar un recurso, como un grupo de reglas de firewall de DNS, una zona alojada privada, una regla de resolutor, etc., a un perfil especificado	Escritura			
CreateProfile	Concede permiso para crear un nuevo recurso de perfil	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteProfile	Otorga permiso para eliminar un perfil especificado por la ProfileId	Escritura			
DisassociateProfile	Concede permiso para eliminar una asociación entre una VPC del cliente y el perfil especificado	Escritura			
DisassociateResour	Concede permiso para eliminar la asociación entre el recurso, como un grupo	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ceFromProfile	de reglas de firewall de DNS, una zona alojada privada, una regla de resolutor, etc., y el perfil especificado				
GetProfile	Concede permiso para obtener un perfil	Lectura			
GetProfileAssociation	Concede permiso para obtener una asociación de perfil a una VPC especificada por el ID de asociación de perfil	Lectura			
GetProfilePolicy [solo permiso]	Concede permiso para leer la política de control de acceso de RAM para un perfil	Lectura	profile*		
GetProfileResourceAssociation	Otorga permiso para obtener una asociación de recursos de perfil basada en ProfileResourceAssociationId	Lectura			
ListProfileAssociations	Otorga permiso para enumerar todos VPCs los perfiles especificados a los que está asociado	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProfileResourceAssociations	Concede permiso para enumerar todas las asociaciones entre los recursos, como grupos de reglas de firewall de DNS, zonas alojadas privadas, reglas de resolutor, etc., para el ID de perfil proporcionado	Enumeración			
ListProfiles	Concede permiso para enumerar todos los perfiles creados por el cliente y compartidos con este	Enumeración			
ListTagsForResource	Concede permiso para enumerar todas las etiquetas asociadas al recurso	Enumeración			
PutProfilePolicy [solo permiso]	Concede permiso para definir la política de control de acceso a la RAM para un perfil	Escritura	profile*		
TagResource	Concede permiso para agregar una etiqueta al recurso proporcionado	Etiquetado	profile		
			profile-association		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar una etiqueta del recurso proporcionado	Etiquetado	profile		
			profile-association		
				aws:TagKeys	
UpdateProfileResourceAssociation	Concede permiso para actualizar el nombre de la asociación de recurso de perfil, las propiedades del recurso, o ambos. Si tanto el nombre como las propiedades del recurso son nulos, la API devuelve la asociación de recurso de perfil existente	Escritura			

Tipos de recursos definidos por Perfiles de Amazon Route 53

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
profile	arn:${Partition}:route53profiles:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
profile-association	arn:${Partition}:route53profiles:${Region}:${Account}:profile-association/${ResourceId}	aws:ResourceTag/${TagKey}

Claves de condición para Perfiles de Amazon Route 53

Perfiles de Amazon Route 53 define las siguientes claves de condición que se pueden usar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la presencia de los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster (prefijo de servicio: `route53-recovery-cluster`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para usarse en las políticas de permiso de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Route 53 Recovery Cluster
- Tipos de recursos definidos por Amazon Route 53 Recovery Cluster
- Claves de condición de Amazon Route 53 Recovery Cluster

Acciones definidas por Amazon Route 53 Recovery Cluster

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRoutingControlState	Otorga permiso para obtener un estado de control de enrutamiento	Lectura	routingcontrol*		
ListRoutingControls	Otorga permiso para enumerar controles de enrutamiento	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRoutingControlState	Otorga permiso para actualizar el estado de control de enrutamiento	Escritura	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	
UpdateRoutingControlStates	Otorga permiso para actualizar un lote de estados de control de enrutamiento	Escritura	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	

Tipos de recursos definidos por Amazon Route 53 Recovery Cluster

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	

Claves de condición de Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
route53-recovery-cluster:AllowSafetyRulesOverrides	Invalidar las reglas de seguridad para permitir las actualizaciones de estado del control de enrutamiento	Bool

Acciones, recursos y claves de condición para Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls (prefijo de servicio: `route53-recovery-control-config`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Route 53 Recovery Controls
- Tipos de recursos definidos por Amazon Route 53 Recovery Controls
- Claves de condición de Amazon Route 53 Recovery Controls

Acciones definidas por Amazon Route 53 Recovery Controls

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCluster	Concede permiso para crear un clúster	Escritura	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateControlPanel	Otorga permiso para crear un panel de control	Escritura	controlpanel*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
CreateRoutingControl	Otorga permiso para crear un control de enrutamiento	Escritura	routingcontrol*		
CreateSafetyRule	Otorga permiso para crear una regla de seguridad	Escritura	safetyrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Otorga permiso para eliminar un clúster	Escritura	cluster*		
DeleteControlPanel	Otorga permiso para eliminar un panel de control	Escritura	controlpanel*		
DeleteResourcePolicy [solo permiso]	Otorga permiso para eliminar la política de control de acceso a la RAM de un clúster	Escritura	cluster*		
DeleteRoutingControl	Otorga permiso para eliminar un control de enrutamiento	Write	routingcontrol*		
DeleteSafetyRule	Otorga permiso para eliminar una regla de seguridad	Write	safetyrule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCluster	Otorga permiso para describir un clúster	Read	cluster*		
DescribeControlPanel	Otorga permiso para describir un panel de control	Read	controlpanel*		
DescribeRoutingControl	Otorga permiso para describir un control de enrutamiento	Read	routingcontrol*		
DescribeRoutingControlByName	Otorga permiso para describir un control de enrutamiento	Read	routingcontrol*		
DescribeSafetyRule	Otorga permiso para describir una regla de seguridad	Lectura	safetyrule*		
GetResourcePolicy	Concede permiso para obtener la política de recursos de un clúster	Lectura	cluster*		
ListAssociatedRoute53HealthChecks	Otorga permiso para enumerar comprobaciones de estado asociadas de Route 53	Enumeración			
ListClusters	Otorga permiso para enumerar clústeres	Lectura			
ListControlPanels	Otorga permiso para enumerar paneles de control	Read			
ListRoutingControls	Otorga permiso para enumerar controles de enrutamiento	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSafetyRules	Otorga permiso para enumerar reglas de seguridad	Lectura	controlpanel*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
PutResourcePolicy [solo permiso]	Otorga permiso para definir la política de control de acceso a la RAM de un clúster	Escritura	cluster*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCluster	Otorga permiso para actualizar un clúster	Escritura	cluster*		
UpdateControlPanel	Otorga permiso para actualizar un clúster	Escritura	controlpanel*		
UpdateRoutingControl	Otorga permiso para actualizar un control de enrutamiento	Escritura	routingcontrol*		
UpdateSafetyRule	Otorga permiso para actualizar una regla de seguridad	Escritura	safetyrule*		

Tipos de recursos definidos por Amazon Route 53 Recovery Controls

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cluster	`arn:${Partition}:route53-recovery-control::${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
controlpanel	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
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}

Claves de condición de Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness (prefijo de servicio: `route53-recovery-readiness`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Route 53 Recovery Readiness
- Tipos de recursos definidos por Amazon Route 53 Recovery Readiness
- Claves de condición de Amazon Route 53 Recovery Readiness

Acciones definidas por Amazon Route 53 Recovery Readiness

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCell	Otorga permiso para crear una celda nueva	Escritura	cell*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCrossAccountAuthorization	Otorga permiso para crear una autorización de cuenta cruzada	Escritura			
CreateReadinessCheck	Otorga permiso para crear una verificación de preparación	Escritura	readinesscheck*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryGroup	Otorga permiso para crear un grupo de recuperación	Escritura	recoverygroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceSet	Otorga permiso para crear un conjunto de recursos	Escritura	resourceset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteCell	Otorga permiso para eliminar una celda	Escritura	cell*		
DeleteCrossAccountAuthorization	Otorga permiso para eliminar una autorización de cuenta cruzada	Escritura			
DeleteReadinessCheck	Otorga permiso para eliminar una verificación de preparación	Escritura	readinesscheck*		
DeleteRecoveryGroup	Otorga permiso para eliminar un grupo de recuperación	Escritura	recoverygroup*		
DeleteResourceSet	Otorga permiso para eliminar un conjunto de recursos	Escritura	resourceset*		
GetArchitectureRecommendations	Otorga permiso para obtener recomendaciones de arquitectura para un grupo de recuperación	Lectura	recoverygroup*		
GetCell	Otorga permiso para obtener información sobre una celda	Lectura	cell*		
GetCellReadinessSummary	Otorga permiso para obtener el resumen de preparación para la celda	Lectura	cell*		
GetReadinessCheck	Otorga permiso para obtener información acerca de una verificación de preparación	Lectura	readinesscheck*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetReadinessCheckResourceStatus	Otorga permiso para obtener el estado de preparación para un recurso individual	Lectura	readinesscheck*		
GetReadinessCheckStatus	Otorga permiso para obtener el estado de una verificación de preparación (para un conjunto de recursos)	Lectura	readinesscheck*		
GetRecoveryGroup	Otorga permiso para obtener información sobre un grupo de recuperación	Lectura	recoverygroup*		
GetRecoveryGroupReadinessSummary	Otorga permiso para obtener el resumen de preparación de un grupo de recuperación	Lectura	recoverygroup*		
GetResourceSet	Otorga permiso para obtener información sobre un conjunto de recursos	Lectura	resourceset*		
ListCells	Otorga permiso para enumerar celdas	Lectura			
ListCrossAccountAuthorizations	Otorga permiso para enumerar autorizaciones de cuentas cruzadas	Lectura			
ListReadinessChecks	Otorga permiso para enumerar verificaciones de preparación	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRecoveryGroups	Otorga permiso para enumerar grupos de recuperación	Lectura			
ListResourceSets	Otorga permiso para enumerar conjuntos de recursos	Lectura			
ListRules	Otorga permiso para enumerar reglas de preparación	Read			
ListTagsForResources	Concede permiso para enumerar las etiquetas de un recurso	Read			
TagResource	Otorga permiso para agregar una etiqueta a un recurso.	Etiquetado	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateCell	Otorga permiso para actualizar una celda	Escritura	cell*		
				aws:TagKeys	
UpdateReadinessCheck	Otorga permiso para actualizar una verificación de preparación	Escritura	readinesscheck*		
				aws:TagKeys	
UpdateRecoveryGroup	Otorga permiso para actualizar un grupo de recuperación	Escritura	recoverygroup*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateResourceSet	Otorga permiso para actualizar un conjunto de recursos	Escritura	resourceset*		
				aws:TagKeys	

Tipos de recursos definidos por Amazon Route 53 Recovery Readiness

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
readinesscheck	`arn:${Partition}:route53-recovery-readiness::${Account}:readiness-check/${ResourceId}`	aws:ResourceTag/${TagKey}
resourceset	`arn:${Partition}:route53-recovery-readiness::${Account}:resource-set/${ResourceId}`	aws:ResourceTag/${TagKey}
cell	`arn:${Partition}:route53-recovery-readiness::${Account}:cell/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
recoverygroup	`arn:${Partition}:route53-recovery-readiness::${Account}:recovery-group/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Route 53 Resolver

Amazon Route 53 Resolver (prefijo de servicio: `route53resolver`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Route 53 Resolver
- Tipos de recursos definidos por Amazon Route 53 Resolver
- Claves de condición para Amazon Route 53 Resolver

Acciones definidas por Amazon Route 53 Resolver

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateFirewallRuleGroup	Otorga permiso para asociar una Amazon VPC a un grupo de reglas de firewall especificado	Write	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	Otorga permiso para asociar una dirección IP especificada con un punto de enlace de Resolver. Se trata de una	Escritura	resolver-endpoint*		ec2:CreateNetworkInterface

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	dirección IP por la que pasan las consultas de DNS cuando se dirigen a su red (saliente) o a la suya VPCs (entrante)				ec2:DescribeNetworkInterfaces ec2:DescribeSubnets
AssociateResolverQueryLogConfig	Otorga permiso para asociar una Amazon VPC con una configuración de registro de consultas especificada	Write	resolver-query-log-config*		ec2:DescribeVpcs
AssociateResolverRule	Otorga permiso para asociar una regla de Resolver especificada con una VPC especificada.	Write	resolver-rule*		ec2:DescribeVpcs
CreateFirewallDomainList	Otorga permiso para crear una lista de dominios de firewall.	Write	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Otorga permiso para crear una regla de firewall dentro de un grupo de reglas de firewall.	Write	firewall-domain-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			firewall-rule-group*		
CreateFirewallRuleGroup	Otorga permiso para crear un grupo de reglas de firewall.	Escritura	firewall-rule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutpostResolver	Otorga permiso para crear un Route 53 Resolver en Outposts	Escritura	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateResolverEndpoint	Otorga permiso para crear un punto enlace de Resolver. Existen dos tipos de puntos de enlace de Resolver: de entrada y de salida.	Escritura	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateResolverQueryLogConfig	Otorga permiso para crear una configuración de registro de consultas de Resolver, que define dónde desea que Resolver guarde los registros de consultas de DNS que se originan en su VPCs	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverRule	Otorga permiso para definir cómo dirigir las consultas que salen de su VPC fuera de la VPC.	Escritura	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	Otorga permiso para eliminar una lista de dominios de firewall.	Write	firewall-domain-list*		
DeleteFirewallRule	Otorga permiso para eliminar una regla de firewall dentro de un grupo de reglas de firewall.	Write	firewall-domain-list*		
			firewall-rule-group*		
DeleteFirewallRuleGroup	Otorga permiso para eliminar un grupo de reglas de firewall.	Escritura	firewall-rule-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteOutpostResolver	Otorga permiso para eliminar un Route 53 Resolver en Outposts	Escritura	outpost-resolver*		
DeleteResolverEndpoint	Otorga permiso para eliminar un punto de enlace de Resolver. El efecto de eliminar un punto de enlace de Resolver depende de si se trata de un punto de enlace de Resolver de entrada o de salida.	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	Otorga permiso para eliminar una configuración de registro de consultas de Resolver	Write	resolver-query-log-config*		
DeleteResolverRule	Otorga permiso para eliminar una regla de Resolver.	Write	resolver-rule*		
DisassociateFirewallRuleGroup	Otorga permiso para quitar la asociación entre un grupo de reglas de firewall especificado y una VPC especificada	Write	firewall-rule-group-association*		
DisassociateResolverEndpointIpAddress	Otorga permiso para eliminar una dirección IP especificada de un punto de enlace de Resolver. Se trata de una dirección IP por la que pasan las consultas de DNS cuando se dirigen a su red (salientes) o a la suya VPCs (entrantes)	Escritura	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateResolverQueryLogConfig	Otorga permiso para eliminar la asociación entre una configuración de registro de consultas de Resolver especificada y una VPC especificada	Write	resolver-query-log-config*		
DisassociateResolverRule	Otorga permiso para eliminar la asociación entre una regla de Resolver especificada y una VPC especificada	Write	resolver-rule*		
GetFirewallConfig	Otorga permiso para obtener información sobre una configuración de firewall especificada.	Read	firewall-config*		ec2:DescribeVpcs
GetFirewallDomainList	Otorga permiso para obtener información sobre una lista de dominios de firewall especificada.	Read	firewall-domain-list*		
GetFirewallRuleGroup	Otorga permiso para obtener información sobre un grupo de reglas de firewall especificado.	Read	firewall-rule-group*		
GetFirewallRuleGroupAssociation	Otorga permiso para obtener información sobre una asociación entre un grupo de reglas de firewall especificado y una VPC	Lectura	firewall-rule-group-association*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFirewallRuleGroupPolicy	Otorga permiso para obtener información sobre una política de grupo de reglas de firewall específica, que especifica las operaciones y los recursos del grupo de reglas de firewall que desea permitir que otro usuario utilice Cuenta de AWS	Lectura	firewall-rule-group*		
GetOutpostResolver	Otorga permiso para obtener información sobre un determinado Route 53 Resolver en Outposts	Lectura	outpost-resolver*		
GetResolverConfig	Otorga permiso para obtener el estado Resolver Config dentro del recurso especificado.	Lectura	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	Otorga permiso para obtener el estado de compatibilidad de validación de las DNSSEC para las consultas DNS dentro del recurso especificado	Read	resolver-dnssec-config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResolverEndpoint	Otorga permiso para obtener información sobre un punto de enlace de Resolver especificado; por ejemplo, si se trata de un punto de enlace de Resolver de entrada o de salida, y las direcciones IP de su VPC a las que se envían las consultas de DNS que entran o salen de su VPC.	Lectura	resolver-endpoint*		
GetResolverQueryLogConfig	Otorga permiso para obtener información sobre una configuración de registro de consultas de Resolver específica, como el número de las VPCs que la configuración registra las consultas y la ubicación a la que se envían los registros	Lectura	resolver-query-log-config*		ec2:DescribeVpcs
GetResolverQueryLogConfigAssociation	Otorga permiso para obtener información sobre una asociación especificada entre una configuración de registro de consultas de Resolver y una Amazon VPC. Cuando asocia una VPC con una configuración de registro de consultas, Resolver registra consultas DNS que se originan en esa VPC	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResolverQueryLogConfigPolicy	Otorga permiso para obtener información sobre una política de registro de consultas de Resolver específica, que especifica las operaciones y los recursos de registro de consultas de Resolver que desea permitir que otra Cuenta de AWS persona utilice	Lectura	resolver-query-log-config*		
GetResolverRule	Otorga permiso para obtener información sobre una regla de resolución especificada, como, por ejemplo, el nombre de dominio al que la regla envía las consultas de DNS y la dirección IP a la que se envían las consultas.	Read	autodefined-rule		
			resolver-rule		
GetResolverRuleAssociation	Otorga permiso para obtener información acerca de una asociación entre una regla de Resolver especificada y una VPC.	Lectura	autodefined-rule		
			resolver-rule		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResolverRulePolicy	Otorga permiso para obtener información sobre una política de reglas de Resolver, que especifica las operaciones y los recursos de Resolver que desea permitir que otro Cuenta de AWS usuario utilice	Lectura	resolver-rule*		
ImportFirewallDomains	Otorga permiso para agregar, quitar o reemplazar dominios de firewall en una lista de dominios de firewall.	Escritura	firewall-domain-list*		
ListFirewallConfigs	Otorga permiso para enumerar todas las configuraciones de firewall Cuenta de AWS que Current puede comprobar	Enumeración			ec2:DescribeVpcs
ListFirewallDomainLists	Otorga permiso para enumerar toda la lista de dominios del Firewall Cuenta de AWS que puede usar Current	Enumeración			
ListFirewallDomains	Otorga permiso para incluir todos los dominios de Firewall en una lista de dominios de Firewall específica	Enumeración	firewall-domain-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFirewallRuleGroupAssociations	Otorga permiso para incluir información sobre las asociaciones entre Amazon VPCs y el grupo de reglas de Firewall	Enumeración			
ListFirewallRuleGroups	Otorga permiso para enumerar todos los grupos de reglas de Firewall que Cuenta de AWS actualmente puede usar	Enumeración			
ListFirewallRules	Otorga permiso para enumerar todas las reglas de firewall de un grupo de reglas de firewall específico	Enumeración	firewall-rule-group*		
ListOutpostResolvers	Otorga permiso para enumerar todas las instancias de Route 53 Resolver en Outposts que se crearon con la versión actual Cuenta de AWS	Enumeración			
ListResolverConfigs	Otorga permiso para enumerar los estados de Resolver Config.	Enumeración	resolver-config*		ec2:DescribeVpcs
ListResolverDnssecConfigs	Otorga permiso para enumerar los estados de compatibilidad de validación de las DNSSEC para las consultas DNS	Enumeración	resolver-dnssec-config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResolverEndpointIpAddresses	Otorga permiso para enumerar las direcciones IP por las que pasan las consultas de DNS cuando se dirigen a su red (salientes) o a la suya VPCs (entrantes) para un punto final de Resolver específico	Enumeración	resolver-endpoint*		
ListResolverEndpoints	Otorga permiso para enumerar todos los puntos finales del Resolver que se crearon con el actual Cuenta de AWS	Enumeración			
ListResolverQueryLogConfigAssociations	Otorga permiso para incluir información sobre las asociaciones entre Amazon VPCs y las configuraciones de registro de consultas	Enumeración			ec2:DescribeVpcs
ListResolverQueryLogConfigs	Otorga permiso para incluir información sobre las configuraciones de registro de consultas especificadas, que definen dónde desea VPCs que Resolver guarde los registros de consultas de DNS y especifican dónde desea registrar las consultas	Enumeración			ec2:DescribeVpcs

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResolverRuleAssociations	Otorga permiso para enumerar las asociaciones que se crearon entre las reglas de Resolver y las que VPCs utilizan las actuales Cuenta de AWS	Enumeración			ec2:DescribeVpcs
ListResolverRules	Otorga permiso para enumerar las reglas de Resolver que se crearon con la actual Cuenta de AWS	Enumeración			
ListTagsForResource	Otorga permiso para obtener una lista de las etiquetas que ha asociado con el recurso especificado	Lectura	firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			resolver-query-log-config		
			resolver-rule		
PutFirewallRuleGroupPolicy	Otorga permiso para especificar con el Cuenta de AWS que desea compartir un grupo de reglas de firewall, el grupo de reglas de firewall que desea compartir y las operaciones que desea que la cuenta pueda realizar en la configuración	Administración de permisos	firewall-rule-group*		
PutResolverQueryLogConfigPolicy	Otorga permiso para especificar una con la Cuenta de AWS que desea compartir una configuración de registro de consultas, la configuración de registro de consultas que desea compartir y las operaciones que desea que la cuenta pueda realizar en la configuración	Administración de permisos	resolver-query-log-config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResolverRulePolicy	Otorga permiso para especificar una con la Cuenta de AWS que desea compartir las reglas, las reglas de Resolver que desea compartir y las operaciones que desea que la cuenta pueda realizar con esas reglas	Administración de permisos	resolver-rule*		
TagResource	Otorga permiso para agregar una o varias etiquetas a un recurso especificado.	Etiquetado	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una o más etiquetas de un recurso especificado.	Etiquetado	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	
UpdateFirewallConfig	Otorga permiso para actualizar la configuración seleccionada para una configuración de firewall.	Write	firewall-config*		ec2:DescribeVpcs
UpdateFirewallDomains	Otorga permiso para agregar, quitar o reemplazar dominios de firewall en una lista de dominios de firewall.	Write	firewall-domain-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFirewallRule	Otorga permiso para actualizar la configuración seleccionada para una regla de firewall en un grupo de reglas de firewall.	Write	firewall-domain-list*		
			firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	Otorga permiso para actualizar la configuración seleccionada para una asociación de grupo de reglas de firewall.	Escritura	firewall-rule-group-association*		
UpdateOutpostResolver	Otorga permiso para actualizar la configuración seleccionada para un Route 53 Resolver específico en Outposts	Escritura	outpost-resolver*		
UpdateResolverConfig	Otorga permiso para actualizar el estado de Resolver Config dentro del recurso especificado.	Escritura	resolver-config*		ec2:DescribeVpcs
UpdateResolverDnssecConfig	Otorga permiso para actualizar el estado de compatibilidad de validación de las DNSSEC para las consultas DNS dentro del recurso especificado	Write	resolver-dnssec-config*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateResolverEndpoint	Otorga permiso para actualizar la configuración seleccionada de un punto de enlace de Resolver de entrada o de salida.	Write	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	Otorga permiso para actualizar la configuración de una regla de Resolver especificada.	Write	resolver-rule*		

Tipos de recursos definidos por Amazon Route 53 Resolver

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
resolver-dnssec-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-dnssec-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-query-log-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-query-log-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-rule	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-rule/${ResourceId}	aws:ResourceTag/${TagKey}
autodefined-rule	arn:${Partition}:route53resolver:${Region}:${Account}:autodefined-rule/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-endpoint	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group-association	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group-association/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-domain-list	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
firewall-config	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-config/${ResourceId}	
outpost-resolver	arn:${Partition}:route53resolver:${Region}:${Account}:outpost-resolver/${ResourceId}	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Route 53 Resolver

Amazon Route 53 Resolver define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la presencia de los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon S3 Express

Amazon S3 Express (prefijo de servicio: `s3express`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para usarlos en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon S3 Express
- Tipos de recurso definidos por Amazon S3 Express
- Claves de condición de Amazon S3 Express

Acciones definidas por Amazon S3 Express

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccessPoint	Concede permiso para crear una aplicación nueva	Write	accesspoint*		
				s3express:DataAccessPointAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBucket	Concede permiso para crear un nuevo bucket	Escritura	bucket*		
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSession	Otorga permiso para crear un token de sesión que se utiliza para objetos APIs como PutObject GetObject, etc.	Escritura	bucket*		
			accesspoint	s3express:Permissions	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:authType s3express:ResourceAccount s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-encryption	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:x-amz-server-side-encryption-aws-kms-key-id s3express:AllAccessRestrictedToLocalZoneGroup s3express:Permissions	
DeleteAccessPoint	Concede permiso para eliminar el punto de acceso nombrado en el URI	Write	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
DeleteAccessPointPolicy	Concede permiso para eliminar la política en un punto de acceso especificado	Administración de permisos	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
DeleteAccessPointScope	Otorga permiso para eliminar la configuración del ámbito en un punto de acceso específico	Administración de permisos	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
DeleteBucket	Concede permiso para eliminar el bucket nombrado en el URI	Write	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
DeleteBucketPolicy	Concede permiso para eliminar la política en un bucket especificado	Administración de permisos	bucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetAccessPoint	Concede permiso para devolver información acerca de la configuración especificada	Lectura	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
GetAccessPointPolicy	Otorga permiso para devolver la política de puntos de acceso asociada al punto de acceso especificado	Lectura	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
GetAccessPointScope	Otorga permiso para devolver la configuración del ámbito asociada al punto de acceso especificado	Lectura	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
GetBucketPolicy	Concede permiso para devolver la política del bucket especificado	Lectura	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEncryptionConfiguration	Concede permiso para devolver la configuración de cifrado predeterminada para un bucket de directorio	Lectura	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLifecycleConfiguration	Otorga permiso para devolver la información de configuración del ciclo de vida establecida en un bucket de directorio	Lectura	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAccessPointsForDirectoryBuckets	Otorga permiso para enumerar puntos de acceso	Enumeración		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAllMyDirectoryBuckets	Concede permiso para enumerar todos los buckets de directorio propiedad del remitente autenticado de la solicitud	Enumeración		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas de un recurso específico	Enumeración	bucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutAccessPointPolicy	Otorga permiso para asociar una política de acceso a un punto de acceso especificado	Administración de permisos	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
PutAccessPointScope	Otorga permiso para asociar un punto de acceso a una configuración de alcance de punto de acceso específica	Administración de permisos	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				content-sha256	
PutBucketPolicy	Otorga permiso para agregar o reemplazar una política de bucket	Administración de permisos	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutEncryptionConfiguration	Concede permiso para establecer la configuración de cifrado para un bucket de directorio	Escritura	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutLifecycleConfiguration	Otorga permiso para crear una nueva configuración de ciclo de vida para el depósito de directorios o reemplazar una configuración de ciclo de vida existente	Escritura	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para crear una nueva etiqueta definida por el usuario o actualizar una etiqueta existente	Etiquetado	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar las etiquetas definidas por el usuario especificadas de un recurso de S3	Etiquetado	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:TagKeys	

Tipos de recurso definidos por Amazon S3 Express

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
bucket	`arn:${Partition}:s3express:${Region}:${Account}:bucket/${BucketName}`	aws:ResourceTag/${TagKey} s3express:BucketTag/${TagKey}
accesspoint	`arn:${Partition}:s3express:${Region}:${Account}:accesspoint/${AccessPointName}`	

Claves de condición de Amazon S3 Express

Amazon S3 Express define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
s3express:AccessPointNetworkOrigin	Filtra el acceso por el origen de la red (Internet o VPC)	Cadena
s3express:AllAccessRestrictedToLocalZoneGroup	Filtra el acceso por los grupos fronterizos de la red de la zona AWS local proporcionados en esta clave de condición	Cadena
s3express:BucketTag/${TagKey}	Filtra el acceso por pares clave-valor de etiqueta adjuntos al bucket	Cadena
s3express:DataAccessPointAccount	Filtra el acceso por el ID de AWS cuenta propietario del punto de acceso	Cadena
s3express:DataAccessPointArn	Filtra el acceso por un punto de acceso Nombre de recurso de Amazon (ARN)	ARN
s3express:LocationName	Filtra el acceso por una zona de disponibilidad específica o un identificador de zona local	Cadena
s3express:Permissions	Filtra el acceso según el permiso solicitado por la configuración de Access Point Scope, por ejemplo GetObject, PutObject	ArrayOfString
s3express:ResourceAccount	Filtra el acceso por el Cuenta de AWS ID del propietario del recurso	Cadena
s3express:SessionMode	Filtra el acceso según el permiso solicitado por la CreateSession API, como ReadOnly y ReadWrite	Cadena

Claves de condición	Descripción	Tipo
s3express:TlsVersion	Filtra el acceso por la versión de TLS utilizada por el cliente	Numérico
s3express:authType	Filtra el acceso por método de autenticación	Cadena
s3express:signatureAge	Filtra el acceso por la antigüedad en milisegundos de la firma de la solicitud	Numérico
s3express:signatureversion	Filtra el acceso según la versión AWS firmada utilizada en la solicitud	Cadena
s3express:x-amz-content-sha256	Filtra el acceso en función del contenido sin firmar en el bucket	Cadena
s3express:x-amz-server-side-encryption	Filtra el acceso por cifrado en el lado del servidor	Cadena
s3express:x-amz-server-side-encryption-aws-kms-key-id	Filtra el acceso mediante la clave administrada por el cliente de AWS KMS para el cifrado del lado del servidor	ARN

Acciones, recursos y claves de condición para Amazon S3 Glacier

Amazon S3 Glacier (prefijo de servicio: `glacier`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para usarlos en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon S3 Glacier
- Tipos de recurso definidos por Amazon S3 Glacier
- Claves de condición de Amazon S3 Glacier

Acciones definidas por Amazon S3 Glacier

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AbortMultipartUpload	Otorga permiso para anular una carga multiparte identificada por el ID de carga	Escritura	vault*		
AbortVaultLock	Otorga permios para anular el bloqueo de almacenes en caso de que el almacén no se encuentre en el estado bloqueado.	Administración de permisos	vault*		
AddTagsToVault	Otorga permiso para agregar etiquetas especificadas a un almacén.	Etiquetado	vault*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CompleteMultipartUpload	Otorga permiso para completar un proceso de carga multiparte.	Escritura	vault*		
CompleteVaultLock	Otorga permiso para completar el proceso de bloqueo de almacenes.	Administración de permisos	vault*		
CreateVault	Otorga permiso para crear un nuevo almacén con el nombre especificado.	Escritura	vault*		
DeleteArchive	Otorga permiso para eliminar un archivo de un almacén.	Escritura	vault*		
				glacier:ArchiveAgeInDays	
DeleteVault	Otorga permiso para eliminar un almacén.	Escritura	vault*		
DeleteVaultAccessPolicy	Otorga permiso para eliminar la política de acceso asociada al almacén especificado.	Administración de permisos	vault*		
DeleteVaultNotifications	Otorga permiso para eliminar la configuración de notificación configurada para un almacén	Escritura	vault*		
DescribeJob	Otorga permiso para obtener información sobre un trabajo iniciado anteriormente.	Lectura	vault*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeVault	Otorga permiso para obtener información sobre un almacén	Lectura	vault*		
GetDataRetrievalPolicy	Otorga permiso para obtener la política de recuperación de datos	Lectura			
GetJobOutput	Otorga permiso para descargar la salida del trabajo especificado.	Lectura	vault*		
GetVaultAccessPolicy	Otorga permiso para recuperar el subrecurso de política de acceso establecido en el almacén.	Lectura	vault*		
GetVaultLock	Otorga permiso para recuperar los atributos del subrecurso de política de bloqueo establecido en el almacén especificado.	Lectura	vault*		
GetVaultNotifications	Otorga permiso para recuperar el subrecurso de configuración de notificaciones establecido en el almacén.	Lectura	vault*		
InitiateJob	Otorga permiso para iniciar un trabajo del tipo especificado.	Escritura	vault*		
				glacier:ArchiveAgeInDays	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
InitiateMultipartUpload	Otorga permiso para iniciar una carga multiparte.	Escritura	vault*		
InitiateVaultLock	Otorga permiso para iniciar el proceso de bloqueo de almacenes.	Administración de permisos	vault*		
ListJobs	Otorga permiso para enumerar los trabajos de un almacén que están en curso y los trabajos que han terminado recientemente.	Enumeración	vault*		
ListMultipartUploads	Otorga permiso para enumerar las cargas multipart e en curso del almacén especificado.	Enumeración	vault*		
ListParts	Otorga permiso para enumerar las partes de un archivo que se han cargado para una carga multiparte específica	Enumeración	vault*		
ListProvisionedCapacity	Otorga permiso para enumerar la capacidad aprovisionada para la especificada Cuenta de AWS	Enumeración			
ListTagsForVault	Otorga permiso para enumerar todas las etiquetas asociadas con un almacén.	Enumeración	vault*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListVaults	Otorga permiso para enumerar todos los almacenes .	Enumeración			
PurchaseProvisionedCapacity	Concede permiso para comprar una unidad de capacidad aprovisionada para un Cuenta de AWS	Escritura			
RemoveTagsFromVault	Otorga permiso para quitar una o varias etiquetas del conjunto de etiquetas asociadas a un almacén.	Etiquetado	vault*		
SetDataRetrievalPolicy	Otorga permiso para establecer y aplicar una política de recuperación de datos en la región especificada en la solicitud PUT.	Administración de permisos			
SetVaultAccessPolicy	Otorga permiso para configurar una política de acceso para un almacén y sobrescribe una política existente.	Administración de permisos	vault*		
SetVaultNotifications	Otorga permiso para configurar notificaciones de almacén.	Escritura	vault*		
UploadArchive	Otorga permiso para cargar un archivo en un almacén.	Escritura	vault*		
UploadMultipartPart	Otorga permiso para cargar una parte de un archivo.	Escritura	vault*		

Tipos de recurso definidos por Amazon S3 Glacier

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Claves de condición de Amazon S3 Glacier

Amazon S3 Glacier define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
glacier:ArchiveAgeInDays	Filtra el acceso mediante el plazo de tiempo que se ha almacenado un archivo en el almacén, en días.	Cadena

Claves de condición	Descripción	Tipo
glacier:ResourceTag/	Filtra el acceso mediante una etiqueta definida por el cliente.	Cadena

Claves de condición, acciones y recursos de Amazon S3 Object Lambda

Amazon S3 Object Lambda (prefijo de servicio: `s3-object-lambda`) brinda los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon S3 Object Lambda
- Tipos de recursos definidos por Amazon S3 Object Lambda
- Claves de condición para Amazon S3 Object Lambda

Acciones definidas por Amazon S3 Object Lambda

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AbortMultipartUpload	Concede permiso para anular una carga multiparte	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObject	Concede permiso para quitar la versión nula de un objeto e insertar un marcador de eliminación, que se convierte en la versión actual del objeto	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:s	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ignatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	Concede permiso para utilizar el subrecurso de etiquetado para quitar todo el conjunto de etiquetas del objeto especificado	Etiquetado	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	Concede permiso para quitar una versión específica de un objeto	Write	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	Concede permiso para quitar todo el conjunto de etiquetas para una versión específica del objeto	Etiquetado	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	Otorga permiso para recuperar objetos de Amazon S3	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	Concede permiso para devolver la lista de control de acceso (ACL) de un objeto	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	Concede permiso para obtener el estado actual de retención legal de un objeto	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	Concede permiso para recuperar la configuración de retención de un objeto	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	Concede permiso para devolver el conjunto de etiquetas de un objeto	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	Concede permiso para recuperar una versión específica de un objeto	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	Concede permiso para devolver la lista de control de acceso (ACL) de una versión de objeto específica	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	Concede permiso para devolver el conjunto de etiquetas para una versión específica del objeto	Read	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	Otorga permiso para enumerar algunos o todos los objetos de un bucket de Amazon S3 (hasta 1000)	List	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	Concede permiso para publicar cargas multiparte en curso	List	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	Concede permiso para enumerar metadatos sobre todas las versiones de objetos en un bucket de Amazon S3	List	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	Concede permiso para enumerar las piezas que se han cargado para una carga multiparte específica	List	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	Otorga permiso para agregar un objeto a un bucket	Escritura	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutObjectAcl	Concede permiso para establecer los permisos de la lista de control de acceso (ACL) para los objetos nuevos o que ya existen en un bucket de S3	Administración de permisos	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	Concede permiso para aplicar una configuración de retención legal al objeto especificado	Write	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	Concede permiso para colocar una configuración de retención de objetos en un objeto	Write	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	Concede permiso para establecer el conjunto de etiquetas suministrado en un objeto que ya existe en un bucket	Etiquetado	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutObjectVersionAcl	Concede permiso para utilizar el subrecurso para establecer los permisos de lista de control de acceso (ACL) para un objeto que ya existe en un bucket	Permissions management	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	Concede permiso para establecer el conjunto de etiquetas suministrado para una versión específica de un objeto	Etiquetado	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	Concede permiso para restaurar una copia archivada de un objeto en Amazon S3	Escritura	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	Otorga permiso para proporcionar datos para GetObject las solicitudes enviadas a S3 Object Lambda	Escritura	objectlambdaaccesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Tipos de recursos definidos por Amazon S3 Object Lambda

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Claves de condición para Amazon S3 Object Lambda

Amazon S3 Object Lambda define las siguientes claves de condición que pueden usarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
s3-object-lambda:TlsVersion	Filtra el acceso por la versión de TLS utilizada por el cliente	Numérico
s3-object-lambda:authType	Filtra el acceso por método de autenticación	Cadena
s3-object-lambda:signatureAge	Filtra el acceso por la antigüedad en milisegundos de la firma de la solicitud	Numérico
s3-object-lambda:versionid	Filtra el acceso por una versión de objeto específica.	Cadena

Acciones, recursos y claves de condición de Amazon S3 en Outposts

Amazon S3 en Outposts (prefijo de servicio: `s3-outposts`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon S3 en Outposts
- Tipos de recursos definidos por Amazon S3 en Outposts
- Claves de condición de Amazon S3 en Outposts

Acciones definidas por Amazon S3 en Outposts

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AbortMultipartUpload	Concede permiso para anular una carga multiparte	Write	object*		
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateAccessPoint	Otorga permiso para crear una aplicación nueva.	Write	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	
CreateBucket	Concede permiso para crear un nuevo bucket	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateEndpoint	Otorga permiso para crear un nuevo punto de enlace	Write	endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccessPoint	Concede permiso para eliminar el punto de acceso nombrado en el URI	Write	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	
DeleteAccessPointPolicy	Concede permiso para eliminar la política en un punto de acceso especificado	Permissions management	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	
DeleteBucket	Concede permiso para eliminar el bucket nombrado en el URI	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBucketPolicy	Concede permiso para eliminar la política en un bucket especificado	Permissions management	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteEndpoint	Otorga permiso para eliminar el punto de enlace nombrado en el URI	Write	endpoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteObject	Concede permiso para quitar la versión nula de un objeto e insertar un marcador de eliminación, que se convierte en la versión actual del objeto	Write	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteObjectTagging	Concede permiso para utilizar el subrecurso de etiquetado para quitar todo el conjunto de etiquetas del objeto especificado	Etiquetado	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteObjectVersion	Concede permiso para quitar una versión específica de un objeto	Write	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteObjectVersionTagging	Concede permiso para quitar todo el conjunto de etiquetas para una versión específica del objeto	Etiquetado	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccessPoint	Otorga permiso para devolver información acerca de la configuración especificada.	Read		s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	
GetAccessPointPolicy	Concede permiso para devolver la política de acceso asociada al punto de acceso especificado	Read	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	
GetBucket	Otorga permiso para devolver la configuración de bucket asociada a un bucket de Amazon S3	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetBucketPolicy	Concede permiso para devolver la política del bucket especificado	Read	bucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBucketTagging	Concede permiso para devolver el conjunto de etiquetas asociado a un bucket de Amazon S3	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBucketVersioning	Concede permiso para devolver el estado de control de versiones de un bucket de Amazon S3	Lectura	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetLifecycleConfiguration	Concede permiso para devolver la información de configuración del ciclo de vida establecida en un bucket de Amazon S3	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObject	Concede permiso para recuperar objetos de Amazon S3	Read	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectTagging	Concede permiso para devolver el conjunto de etiquetas de un objeto	Read	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectVersion	Concede permiso para recuperar una versión específica de un objeto	Lectura	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	
GetObjectVersionForReplication	Concede permiso para replicar objetos no cifrados y objetos cifrados con SSE-KMS	Lectura	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetObjectVersionTagging	Concede permiso para devolver el conjunto de etiquetas para una versión específica del objeto	Read	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetReplicationConfiguration	Concede permiso para obtener la información de configuración de replicación establecida en un bucket de Amazon S3	Lectura	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAccessPoints	Otorga permiso para enumerar puntos de acceso	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucket	Concede permiso para enumerar algunos o todos los objetos de un bucket de Amazon S3 (hasta 1000)	List	accesspoint* bucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucketMultipartUploads	Concede permiso para publicar cargas multiparte en curso	List	accesspoint* bucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBucketVersions	Concede permiso para enumerar metadatos sobre todas las versiones de objetos en un bucket de Amazon S3	Enumeración	bucket*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outpos	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ts:max-keys s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListEndpoints	Concede permiso para enumerar puntos de enlace	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMultipartUploadParts	Concede permiso para enumerar las piezas que se han cargado para una carga multiparte específica	Enumeración	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ureversion s3-outposts:x-amz-content-sha256	
ListOutpostsWithS3	Concede permiso para enumerar outposts con capacidad de S3	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRegionalBuckets	Concede permiso para enumerar todos los buckets propiedad del remitente autenticado de la solicitud	Enumeración		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListSharedEndpoints	Concede permiso para enumerar los puntos de conexión compartidos	Enumeración			
PutAccessPointPolicy	Otorga permiso para asociar una política de acceso a un punto de acceso especificado	Permissions management	accesspoint*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:x-amz-content-sha256	
PutBucketPolicy	Otorga permiso para agregar o reemplazar una política de bucket	Permissions management	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutBucketTagging	Otorga permiso para agregar un conjunto de etiquetas a un bucket existente de Amazon S3	Etiquetado	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutBucketVersioning	Concede permiso para establecer el estado de control de versiones de un bucket de Amazon S3 existente	Escritura	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutLifecycleConfiguration	Concede permiso para crear una nueva configuración de ciclo de vida para el bucket o reemplazar una configuración de ciclo de vida existente	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutObject	Otorga permiso para agregar un objeto a un bucket	Write	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:RequestObjectTag/<key> s3-outposts:RequestObjectTagKeys s3-outpos	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-copy-source s3-outposts:x-amz-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				metadata-directive s3-outposts:x-amz-server-side-encryption s3-outposts:x-amz-storage-class	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutObjectAcl	Establece los permisos de la lista de control de acceso (ACL) para un objeto que ya existe en un bucket.	Permissions management	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-storage-class	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutObjectTagging	Otorga permiso para establecer el conjunto de etiquetas suministrado en un objeto que ya existe en un bucket	Etiquetado	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
		Etiquetado	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutObjectVersionTagging	Concede permiso para establecer el conjunto de etiquetas suministrado para una versión específica de un objeto			s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key> s3-outposts:Reques	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				tObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	
PutReplicationConfiguration	Concede permiso para crear una nueva configuración de replicación o reemplazar una existente	Escritura	bucket*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
Replicate Delete	Concede permiso para replicar marcadores de eliminación en el bucket de destino	Write	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
Replicate Object	Concede permiso para replicar objetos y etiquetas de objeto en el bucket de destino	Write	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-server-side-encryption	
ReplicateTags	Concede permiso para replicar etiquetas de objeto en el bucket de destino	Etiquetado	object*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Tipos de recursos definidos por Amazon S3 en Outposts

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
accesspoint	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/accesspoint/${AccessPointName}`	
bucket	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}`	
endpoint	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/endpoint/${EndpointId}`	
object	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}/object/${ObjectName}`	

Claves de condición de Amazon S3 en Outposts

Amazon S3 en Outposts define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
s3-outposts:AccessPointNetworkOrigin	Filtra el acceso por el origen de la red (Internet o VPC)	Cadena

Claves de condición	Descripción	Tipo
s3-outposts:DataAccessPointAccount	Filtra el acceso por el ID de AWS cuenta propietario del punto de acceso	Cadena
s3-outposts:DataAccessPointArn	Filtra el acceso por un punto de acceso Nombre de recurso de Amazon (ARN)	ARN
s3-outposts:ExistingObjectTag/<key>	Filtra el acceso al requerir que una etiqueta de objeto existente tenga una clave y un valor de etiqueta específicos	Cadena
s3-outposts:RequestObjectTag/<key>	Filtra el acceso al restringir las claves y los valores de etiqueta permitidos en los objetos	Cadena
s3-outposts:RequestObjectTagKeys	Filtra el acceso al restringir las claves de etiqueta permitidas en los objetos	Cadena
s3-outposts:authType	Filtra el acceso al restringir las solicitudes entrantes a un método de autenticación específico	Cadena
s3-outposts:delimiter	Filtra el acceso al requerir el parámetro delimitador	Cadena
s3-outposts:max-keys	Filtra el acceso limitando el número máximo de claves devueltas en una ListBucket solicitud	Numérico
s3-outposts:prefix	Filtra el acceso por prefijo de nombre de clave	Cadena

Claves de condición	Descripción	Tipo
s3-outposts:signatureAge	Filtra el acceso al identificar el periodo, en milisegundos, que una firma es válida en una solicitud autenticada	Numérico
s3-outposts:signatureversion	Filtra el acceso identificando la versión de AWS Signature que se admite en las solicitudes autenticadas	Cadena
s3-outposts:versionid	Filtra el acceso por una versión de objeto específica.	Cadena
s3-outposts:x-amz-acl	Filtra el acceso al requerir que el x-amz-acl encabezado contenga una ACL predefinida específica en una solicitud	Cadena
s3-outposts:x-amz-content-sha256	Filtra el acceso al rechazar el contenido no firmado en el bucket	Cadena
s3-outposts:x-amz-copy-source	Filtra el acceso al restringir el origen de copia a un bucket, prefijo u objeto específicos	Cadena
s3-outposts:x-amz-metadata-directive	Filtra el acceso al habilitar la aplicación del comportamiento de metadatos de objeto (COPIAR o REMPLAZAR) cuando se copian objetos	Cadena
s3-outposts:x-amz-server-side-encryption	Filtra el acceso al requerir el cifrado en el lado del servidor	Cadena
s3-outposts:x-amz-storage-class	Filtra el acceso por clase de almacenamiento.	Cadena

Claves de condición, recursos y acciones para Amazon S3 Tables

Amazon S3 Tables (prefijo de servicio:`s3tables`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las tablas de Amazon S3
- Tipos de recursos definidos por las tablas de Amazon S3
- Claves de condición para las tablas de Amazon S3

Acciones definidas por las tablas de Amazon S3

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNamespace	Otorga permiso para crear un espacio de nombres	Escritura	TableBucket*		
CreateTable	Concede permiso para crear una tabla	Escritura	TableBucket*		
				s3tables:namespace	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				s3tables:SSEAlgorithm s3tables:KMSKeyAr	
CreateTableBucket	Otorga permiso para crear un conjunto de tablas	Escritura	TableBucket*		
				s3tables:SSEAlgorithm s3tables:KMSKeyAr	
DeleteNamespace	Otorga permiso para eliminar un espacio de nombres	Escritura	TableBucket*		
				s3tables:namespace	
DeleteTable	Concede permiso para eliminar una tabla	Escritura	Table*		
				s3tables:namespace s3tables:tableName	
DeleteTableBucket	Otorga permiso para eliminar un cubo de tabla	Escritura	TableBucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTableBucketEncryption	Otorga permiso para eliminar la configuración de cifrado de un cubo de mesa	Escritura	TableBucket*		
DeleteTableBucketPolicy	Otorga permiso para eliminar una política de un cubo de mesa	Administración de permisos	TableBucket*		
DeleteTablePolicy	Otorga permiso para eliminar una política de una tabla	Administración de permisos	Table*		
				s3tables:namespace s3tables:tableName	
GetNamespace	Otorga permiso para obtener un espacio de nombres	Lectura	TableBucket*		
				s3tables:namespace	
GetTable	Concede permiso para recuperar una tabla	Lectura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableBucket	Otorga permiso para recuperar un cubo de mesa	Lectura	TableBucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTableBucketEncryption	Otorga permiso para recuperar la configuración de cifrado de un cubo de mesa	Lectura	TableBucket*		
GetTableBucketMaintenanceConfiguration	Otorga permiso para recuperar una configuración de mantenimiento en un cubo de mesa	Lectura	TableBucket*		
GetTableBucketPolicy	Otorga permiso para recuperar una política de un cubo de mesa	Lectura	TableBucket*		
GetTableData [solo permiso]	Otorga permiso para leer metadatos y objetos de datos de un punto final de almacenamiento de tablas mediante S3 APIs	Lectura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableEncryption	Otorga permiso para recuperar la configuración de cifrado de una tabla	Lectura	Table*		
				s3tables:namespace s3tables:tableName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTableMaintenanceConfiguration	Otorga permiso para recuperar una configuración de mantenimiento de una tabla	Lectura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMaintenanceJobStatus	Otorga permiso para recuperar el estado de los trabajos de mantenimiento de una tabla	Lectura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMetadataLocation	Otorga permiso para recuperar la ubicación de los metadatos de una tabla	Lectura	Table*		
				s3tables:namespace s3tables:tableName	
GetTablePolicy	Otorga permiso para recuperar una política de una tabla	Lectura	Table*		
				s3tables:namespace s3tables:tableName	
ListNamespaces	Otorga permiso para enumerar los espacios de nombres	Enumeración	TableBucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTableBuckets	Otorga permiso para enumerar grupos de tablas	Enumeración			
ListTables	Otorga permiso para enumerar tablas	Enumeración	TableBucket*		
				s3tables:namespace	
PutTableBucketEncryption	Otorga permiso para colocar o sobrescribir la configuración de cifrado en un cubo de mesa	Escritura	TableBucket*		
				s3tables:KMSKeyAr s3tables:SSEAlgorithm	
PutTableBucketMaintenanceConfiguration	Otorga permiso para colocar una configuración de mantenimiento en un cubo de mesa	Escritura	TableBucket*		
PutTableBucketPolicy	Otorga permiso para crear o sobrescribir una política en un cubo de mesa	Administración de permisos	TableBucket*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutTableData [solo permiso]	Otorga permiso para escribir metadatos y objetos de datos en un punto final de almacenamiento de tablas mediante S3 APIs	Escritura	Table*		
				s3tables:namespace s3tables:tableName	
PutTableEncryption [solo permiso]	Otorga permiso para colocar la configuración de cifrado en una tabla	Escritura	Table*		
				s3tables:namespace s3tables:SSEAlgorithm s3tables:KMSKeyAr	
PutTableMaintenanceConfiguration	Otorga permiso para colocar una configuración de mantenimiento en una tabla	Escritura	Table*		
				s3tables:namespace s3tables:tableName	
PutTablePolicy	Otorga permiso para crear o sobrescribir una política en una tabla	Administración de permisos	Table*		
				s3tables:namespace s3tables:tableName	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RenameTable	Otorga permiso para cambiar el nombre de una tabla o moverla entre espacios de nombres	Escritura	Table*		
				s3tables:namespace s3tables:tableName	
UpdateTableMetadataLocation	Otorga permiso para actualizar la ubicación de los metadatos de una tabla	Escritura	Table*		
				s3tables:namespace s3tables:tableName	

Tipos de recursos definidos por las tablas de Amazon S3

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
TableBucket	`arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}`	

Tipos de recurso	ARN	Claves de condición
Table	`arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}/table/${TableID}`	s3tables:namespace s3tables:tableName

Claves de condición para las tablas de Amazon S3

Amazon S3 Tables define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
s3tables:KMSKeyArn	Filtra el acceso mediante la clave de AWS KMS (ARN) para la clave utilizada para cifrar una tabla	ARN
s3tables:SSEAlgorithm	Filtra el acceso mediante el algoritmo de cifrado del lado del servidor utilizado para cifrar una tabla	Cadena
s3tables:namespace	Filtra el acceso por los espacios de nombres creados en el depósito de tablas	Cadena
s3tables:tableName	Filtra el acceso por el nombre de las tablas del cubo de tablas	Cadena

Claves de condiciones, recursos y acciones del asistente de ciencia SageMaker de datos de Amazon

El asistente de ciencia de SageMaker datos de Amazon (prefijo de servicio:`sagemaker-data-science-assistant`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el asistente de ciencia SageMaker de datos de Amazon
- Tipos de recursos definidos por el asistente de ciencia SageMaker de datos de Amazon
- Claves de condición del asistente de ciencia SageMaker de datos de Amazon

Acciones definidas por el asistente de ciencia SageMaker de datos de Amazon

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendConversation [solo permiso]	Concede permiso para iniciar una conversación con el asistente de ciencia SageMaker de datos	Escritura			

Tipos de recursos definidos por el asistente de ciencia SageMaker de datos de Amazon

El asistente SageMaker de ciencia de datos de Amazon no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso al asistente de ciencia SageMaker de datos de Amazon, `"Resource": "*"` especifíquelo en su política.

Claves de condición del asistente de ciencia SageMaker de datos de Amazon

SageMakerDataScienceAssistant no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condiciones, recursos y acciones para las capacidades SageMaker geoespaciales de Amazon

Las capacidades SageMaker geoespaciales de Amazon (prefijo de servicio:`sagemaker-geospatial`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las capacidades SageMaker geoespaciales de Amazon
- Tipos de recursos definidos por las capacidades SageMaker geoespaciales de Amazon
- Claves de condición para las capacidades SageMaker geoespaciales de Amazon

Acciones definidas por las capacidades SageMaker geoespaciales de Amazon

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEarthObservationJob	Otorga permiso a la DeleteEarthObservationJob operación, lo que elimina un trabajo de observación terrestre existente	Escritura	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
DeleteVectorEnrichmentJob	Concede permiso a la DeleteVectorEnrichmentJob operación que elimina un trabajo de enriquecimiento vectorial existente	Escritura	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ExportEarthObservationJob	Otorga permiso para copiar los resultados de un trabajo de observación de la Tierra a una ubicación de S3	Escritura	EarthObservationJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
ExportVectorEnrichmentJob	Otorga permiso para copiar los resultados de an VectorEnrichmentJob a una ubicación S3	Escritura	VectorEnrichmentJob*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetEarthObservationJob	Otorga permiso para devolver detalles sobre el trabajo de observación de la Tierra	Lectura	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
GetRasterDataCollection	Otorga permiso para devolver detalles sobre la recopilación de datos ráster	Lectura	RasterDataCollection*		
				aws:ResourceTag/${TagKey}	
GetTile	Otorga permiso para obtener el icono de un trabajo de observación de la Tierra	Lectura	EarthObservationJob*		iam:PassRole
GetVectorEnrichmentJob	Otorga permiso para devolver detalles sobre el trabajo de enriquecimiento vectorial	Lectura	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEarthObservationJobs	Otorga permiso para devolver una matriz de trabajos de observación de la Tierra asociados a la cuenta actual	Enumeración			
ListRasterDataCollections	Otorga permiso para devolver una matriz de colecciones de datos aster asociados con el nombre del modelo especificado	Enumeración			
ListTagsForResource	Otorga permiso a la etiqueta de listas de un SageMaker recurso geoespacial	Enumeración	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:ResourceTag/${TagKey}	
ListVectorEnrichmentJobs	Otorga permiso para devolver una matriz de trabajos de enriquecimiento vectorial asociados a la cuenta actual	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchRasterDataCollection	Otorga permiso para consultar colecciones de datos ráster	Lectura			
StartEarthObservationJob	Otorga permiso a la StartEarthObservationJob operación que inicia una nueva tarea de observación de la Tierra en su cuenta	Escritura	EarthObservationJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVectorEnrichmentJob	Concede permiso a la StartVectorEnrichmentJob operación que inicia un nuevo trabajo de enriquecimiento vectorial en tu cuenta	Escritura	VectorEnrichmentJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopEarthObservationJob	Otorga permiso a la StopEarthObservationJob operación que detiene un trabajo de observación terrestre existente	Escritura	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
StopVectorEnrichmentJob	Concede permiso a la StopVectorEnrichmentJob operación que detiene un trabajo de enriquecimiento vectorial existente	Escritura	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
TagResource	Otorga permiso para etiquetar un recurso SageMaker geoespacial	Etiquetado	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para desetiquetar un recurso geoespacial SageMaker	Etiquetado	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys	

Tipos de recursos definidos por las capacidades SageMaker geoespaciales de Amazon

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
EarthObservationJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:earth-observation-job/${JobID}`	aws:ResourceTag/${TagKey}
RasterDataCollection	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:raster-data-collection/${CollectionID}`	aws:ResourceTag/${TagKey}
VectorEnrichmentJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:vector-enrichment-job/${JobID}`	aws:ResourceTag/${TagKey}

Claves de condición para las capacidades SageMaker geoespaciales de Amazon

Las capacidades SageMaker geoespaciales de Amazon definen las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon SageMaker con MLflow

Amazon SageMaker con MLflow (prefijo de servicio:`sagemaker-mlflow`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon SageMaker con MLflow
- Tipos de recursos definidos por Amazon SageMaker con MLflow
- Claves de estado para Amazon SageMaker con MLflow

Acciones definidas por Amazon SageMaker con MLflow

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AccessUI	Otorga permiso para acceder a la interfaz de usuario MLflow	Lectura			
CreateExperiment	Otorga permiso para crear un MLflow experimento	Escritura	mlflow-tracking-server*		
CreateModelVersion	Concede permiso para crear una nueva versión de modelo	Escritura	mlflow-tracking-server*		
CreateRegisteredModel	Concede permiso para crear un modelo registrado	Escritura	mlflow-tracking-server*		
CreateRun	Concede permiso para crear una nueva ejecución dentro de un experimento	Escritura	mlflow-tracking-server*		
DeleteExperiment	Otorga permiso para marcar un MLflow experimento para eliminarlo	Escritura	mlflow-tracking-server*		
DeleteModelVersion	Concede permiso para eliminar una versión de modelo	Escritura	mlflow-tracking-server*		
DeleteModelVersionTag	Concede permiso para eliminar una etiqueta de una versión de modelo	Escritura	mlflow-tracking-server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRegisteredModel	Concede permiso para eliminar un modelo registrado	Escritura	mlflow-tracking-server*		
DeleteRegisteredModelAlias	Concede permiso para eliminar un alias de modelo registrado	Escritura	mlflow-tracking-server*		
DeleteRegisteredModelTag	Concede permiso para eliminar una etiqueta de modelo registrado	Escritura	mlflow-tracking-server*		
DeleteRun	Concede permiso para marcar una ejecución para su eliminación	Escritura	mlflow-tracking-server*		
DeleteTag	Concede permiso para eliminar una etiqueta en una ejecución	Escritura	mlflow-tracking-server*		
DeleteTraceTag	Otorga permiso para eliminar una etiqueta de rastreo en MLflow	Escritura	mlflow-tracking-server*		
DeleteTraces	Otorga permiso para eliminar los rastros en MLflow	Escritura	mlflow-tracking-server*		
EndTrace	Otorga permiso para finalizar un rastreo MLflow	Escritura	mlflow-tracking-server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDownloadURIForModelVersionArtifacts	Concede permiso para obtener un URI para descargar artefactos de modelo para una versión específica del modelo	Lectura	mlflow-tracking-server*		
GetExperiment	Otorga permiso para obtener los metadatos de un MLflow experimento	Lectura	mlflow-tracking-server*		
GetExperimentByName	Otorga permiso para obtener los metadatos de un MLflow experimento por su nombre	Lectura	mlflow-tracking-server*		
GetLatestModelVersions	Concede permiso para obtener las versiones más recientes del modelo	Enumeración	mlflow-tracking-server*		
GetMetricHistory	Concede permiso para obtener una lista de todos los valores de la métrica especificada para una ejecución determinada	Lectura	mlflow-tracking-server*		
GetModelVersion	Concede permiso para obtener una versión del modelo según el nombre y la versión	Lectura	mlflow-tracking-server*		
GetModelVersionByAlias	Otorga permiso para obtener la versión del modelo por alias en MLflow	Lectura	mlflow-tracking-server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRegisteredModel	Concede permiso para obtener un modelo registrado	Lectura	mlflow-tracking-server*		
GetRun	Concede permiso para obtener metadatos, métricas, parámetros y etiquetas para una ejecución	Lectura	mlflow-tracking-server*		
GetTraceInfo	Otorga permiso para obtener información sobre un rastreo en MLflow	Lectura	mlflow-tracking-server*		
ListArtifacts	Concede permiso para enumerar artefactos para una ejecución	Enumeración	mlflow-tracking-server*		
LogBatch	Concede permiso para registrar un lote de métricas, parámetros y etiquetas para una ejecución	Escritura	mlflow-tracking-server*		
LogInputs	Concede permiso para registrar entradas para una ejecución	Escritura	mlflow-tracking-server*		
LogMetric	Concede permiso para registrar una métrica para una ejecución	Escritura	mlflow-tracking-server*		
LogModel	Concede permiso para registrar el modelo asociado a una ejecución	Escritura	mlflow-tracking-server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
LogParam	Concede permiso para registrar un parámetro rastreado durante una ejecución	Escritura	mlflow-tracking-server*		
RenameRegisteredModel	Concede permiso para cambiar el nombre de un modelo registrado	Escritura	mlflow-tracking-server*		
RestoreExperiment	Concede permiso para restaurar un experimento marcado para eliminación	Escritura	mlflow-tracking-server*		
RestoreRun	Concede permiso para restaurar una ejecución eliminada	Escritura	mlflow-tracking-server*		
SearchExperiments	Otorga permiso para buscar MLflow experimentos	Lectura	mlflow-tracking-server*		
SearchModelVersions	Concede permiso para buscar una versión de modelo	Lectura	mlflow-tracking-server*		
SearchRegisteredModels	Otorga permiso para buscar modelos registrados en MLflow	Lectura	mlflow-tracking-server*		
SearchRuns	Concede permiso para buscar ejecuciones que cumplan con las expresiones	Lectura	mlflow-tracking-server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SearchTraces	Otorga permiso para buscar rastros en MLflow	Lectura	mlflow-tracking-server*		
SetExperimentTag	Concede permiso para establecer una etiqueta en un experimento	Escritura	mlflow-tracking-server*		
SetModelVersionTag	Concede permiso para establecer una etiqueta para la versión del modelo	Escritura	mlflow-tracking-server*		
SetRegisteredModelAlias	Concede permiso para establecer un alias de modelo registrado	Escritura	mlflow-tracking-server*		
SetRegisteredModelTag	Concede permiso para establecer una etiqueta para un modelo registrado	Escritura	mlflow-tracking-server*		
SetTag	Concede permiso para establecer una etiqueta en una ejecución	Escritura	mlflow-tracking-server*		
SetTraceTag	Otorga permiso para establecer una etiqueta de rastreo MLflow	Escritura	mlflow-tracking-server*		
StartTrace	Otorga permiso para iniciar un rastreo MLflow	Escritura	mlflow-tracking-server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TransitionModelVersionStage	Concede permiso para realizar la transición de una versión del modelo a una etapa determinada	Escritura	mlflow-tracking-server*		
UpdateExperiment	Otorga permiso para actualizar los metadatos de un MLflow experimento	Escritura	mlflow-tracking-server*		
UpdateModelVersion	Concede permiso para actualizar la versión del modelo	Escritura	mlflow-tracking-server*		
UpdateRegisteredModel	Concede permiso para actualizar un modelo registrado	Escritura	mlflow-tracking-server*		
UpdateRun	Concede permiso para actualizar los metadatos de la ejecución	Escritura	mlflow-tracking-server*		

Tipos de recursos definidos por Amazon SageMaker con MLflow

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
mlflow-tracking-server	`arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Claves de estado para Amazon SageMaker con MLflow

Amazon SageMaker with MLflow define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena
sagemaker:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta.	Cadena

Acciones, recursos y claves de condición para AWS Savings Plans

AWS Savings Plans (prefijo de servicio:`savingsplans`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Savings Plans
- Tipos de recursos definidos por AWS Savings Plans
- Claves de condición para AWS Savings Plans

Acciones definidas por AWS Savings Plans

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSavingsPlan	Otorga permisos para crear un plan de ahorro	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Otorga permiso para eliminar el plan de ahorros en cola asociado a la cuenta de clientes	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSavingsPlanRates	Otorga permisos para describir las tarifas asociadas con el plan de ahorro de los clientes	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	Otorga permisos para describir los Savings Plans asociados con la cuenta de clientes	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Otorga permisos para describir las tarifas asignadas con las ofertas de los Savings Plans	Read			
DescribeSavingsPlansOfferings	Otorga permisos para describir las ofertas de los Savings Plans que el cliente puede adquirir	Read			
ListTagsForResource	Otorga permisos para obtener una lista de etiquetas para un plan de ahorro.	Enumeración	savingsplan*		
ReturnSavingsPlan	Concede permiso para devolver un Savings Plan	Escritura	savingsplan*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permisos para etiquetar un plan de ahorro	Etiquetado	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permisos para desetiquetar un plan de ahorro	Etiquetado	savingsplan*		
				aws:TagKeys	

Tipos de recursos definidos por AWS Savings Plans

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Savings Plans

AWS Savings Plans define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el par etiqueta-valor asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Secrets Manager

AWS Secrets Manager (prefijo de servicio:`secretsmanager`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Secrets Manager
- Tipos de recursos definidos por AWS Secrets Manager
- Claves de condición para AWS Secrets Manager

Acciones definidas por AWS Secrets Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetSecretValue	Concede permiso para recuperar y descifrar una lista de secretos	Enumeración			
CancelRotateSecret	Concede permiso para cancelar una rotación secreta en curso	Escritura	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretPrimaryRegion	
CreateSecret	Otorga permiso para crear un secreto que almacena datos cifrados que se puede consultar y rotar.	Escritura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:Add	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ReplicaRegions secretsmanager:ForceOverwriteReplicaSecret	
DeleteResourcePolicy	Otorga permiso para eliminar la política de recursos adjunta a un secreto.	Administración de permisos	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
DeleteSecret	Otorga permiso para eliminar un secreto.	Escritura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				retPrimaryRegion	
DescribeSecret	Otorga permiso para recuperar los metadatos acerca de un secreto, pero no los datos cifrados.	Lectura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetRandomPassword	Otorga permiso para generar una cadena aleatoria para su uso en la creación de contraseñas.	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourcePolicy	Otorga permiso para obtener la política de recursos asociada a un secreto.	Lectura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue	Otorga permiso para recuperar y descifrar los datos cifrados.	Lectura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSecretVersionIds	Otorga permiso para enumerar las versiones disponibles de un secreto.	Lectura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecrets	Otorga permiso para enumerar los secretos disponibles.	Enumeración			
PutResourcePolicy	Otorga permiso para asociar una política de recursos a un secreto.	Administración de permisos	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	
PutSecretValue	Otorga permiso para crear una nueva versión del secreto con nuevos datos cifrados.	Escritura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	Otorga permiso para eliminar regiones de replicación.	Escritura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ReplicateSecretToRegions	Otorga permiso para convertir un secreto existente en un secreto de varias regiones y comienza a replicar el secreto en una lista de regiones nuevas.	Escritura	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions secretsmanager:For	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ceOverwriteReplicaSecret	
RestoreSecret	Otorga permiso para cancelar la eliminación de un secreto.	Escritura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RotateSecret	Otorga permiso para iniciar la rotación de un secreto.	Escritura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaAn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:Mod	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ifyRotationRules secretsmanager:RotateImmediately	
StopReplicationToReplica	Otorga permiso para eliminar el secreto de la reproducción y promueve el secreto a un secreto regional en la región de la réplica.	Escritura	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar etiquetas a un secreto.	Etiquetado	Secret*	secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar etiquetas de un secreto.	Etiquetado	Secret*		
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UpdateSecret	Otorga permiso para actualizar un secreto con metadatos nuevos o con una nueva versión de los datos cifrados.	Escritura	Secret*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				retPrimaryRegion	
UpdateSecretVersionStage	Otorga permiso para mover una fase de un secreto a otro.	Escritura	Secret*	secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ValidateResourcePolicy	Otorga permiso para validar una política de recursos antes de adjuntar la política.	Administración de permisos	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Tipos de recursos definidos por AWS Secrets Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn

Claves de condición para AWS Secrets Manager

AWS Secrets Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave que está presente en la solicitud que el usuario realiza al servicio Secrets Manager.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso mediante la lista de todos los nombres de clave de etiqueta presentes en la solicitud que el usuario realiza al servicio Secrets Manager.	ArrayOfString
secretsmanager:AddReplicaRegions	Filtra el acceso mediante la lista de las regiones en las que se va a replicar el secreto.	ArrayOfString
secretsmanager:BlockPublicPolicy	Filtra el acceso en función de si la política de recursos bloquea el Cuenta de AWS acceso amplio	Bool
secretsmanager:Description	Filtra el acceso mediante el texto de descripción de la solicitud.	Cadena
secretsmanager:ForceDeleteWithoutRecovery	Filtra el acceso en función de si el secreto se debe eliminar de inmediato sin ventana de recuperación.	Bool
secretsmanager:ForceOverwriteReplicaSecret	Filtra el acceso en función de si se debe sobrescribir un secreto con el mismo nombre en la región de destino.	Bool
secretsmanager:KmsKeyArn	Filtra el acceso por la clave ARN de la clave KMS de la solicitud	ARN

Claves de condición	Descripción	Tipo
secretsmanager:KmsKeyId	Filtra el acceso por el identificador clave de la clave KMS de la solicitud. En desuso: utilice el administrador de secretos: KmsKeyArn	Cadena
secretsmanager:ModifyRotationRules	Filtra el acceso en función de si las reglas de rotación del secreto tienen que modificarse.	Bool
secretsmanager:Name	Filtra el acceso mediante el nombre fácil de recordar del secreto de la solicitud.	Cadena
secretsmanager:RecoveryWindowInDays	Filtra el acceso mediante el número de días que Secrets Manager espera antes de poder eliminar el secreto.	Numérico
secretsmanager:ResourceTag/tag-key	Filtra el acceso por par de clave y valor de etiqueta.	Cadena
secretsmanager:RotateImmediately	Filtra el acceso en función de si el secreto debe rotarse inmediatamente.	Bool
secretsmanager:RotationLambdaARN	Filtra el acceso mediante el ARN de la función de Lambda de rotación de la solicitud.	ARN
secretsmanager:SecretId	Filtra el acceso mediante el valor de SecretID de la solicitud.	ARN

Claves de condición	Descripción	Tipo
secretsmanager:SecretPrimaryRegion	Filtra el acceso mediante la región principal en la que se crea el secreto.	Cadena
secretsmanager:VersionId	Filtra el acceso mediante el identificador único de la versión del secreto de la solicitud.	Cadena
secretsmanager:VersionStage	Filtra el acceso mediante la lista de las fases de versión de la solicitud.	Cadena
secretsmanager:resource/AllowRotationLambdaArn	Filtra el acceso mediante el ARN de la función de Lambda de rotación asociada al secreto.	ARN

Acciones, recursos y claves de condición para AWS Security Hub

AWS Security Hub (prefijo de servicio:`securityhub`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Security Hub
- Tipos de recursos definidos por AWS Security Hub

- Claves de condición para AWS Security Hub

Acciones definidas por AWS Security Hub

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptAdministratorInvitation	Concede permiso para aceptar invitaciones de Security Hub para convertirse en una cuenta de miembro.	Write	hub		
AcceptInvitation	Concede permiso para aceptar invitaciones de Security Hub para convertirse en una cuenta de miembro.	Escritura	hub		
BatchDeleteAutomationRules	Concede permiso para eliminar una o varias reglas de automatización en Security Hub	Escritura	automation-rule*		
BatchDisableStandards	Concede permiso para desactivar estándares en Security Hub.	Write	hub		
BatchEnableStandards	Concede permiso para habilitar estándares en Security Hub.	Escritura	hub		
BatchGetAutomationRules	Otorga permiso para recuperar una lista de detalles de las reglas de automatiz	Lectura	automation-rule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	ación de Security Hub en función de la regla Amazon Resource Names (ARNs)				
BatchGetConfigurationPolicyAssociations	Concede permiso para recuperar información sobre las políticas de configuración asociadas a una lista específica de cuentas de miembros y unidades organizacionales de la organización de la cuenta que realiza la llamada	Lectura			
BatchGetControlEvaluations [solo permiso]	Concede permiso para obtener el estado de habilitación y cumplimiento de los controles, el número de resultados de los controles y la puntuación general de seguridad de los controles en la consola de Security Hub	Lectura	hub		
BatchGetSecurityControls	Concede permiso para obtener detalles sobre controles de seguridad específicos identificados por ID o ARN	Lectura			securityhub:DescribeStandardsControls
BatchGetStandardsControlAssociations	Concede permiso para obtener el estado de habilitación de un lote de controles de seguridad en estándares	Lectura			securityhub:DescribeStandardsControls

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchImportFindings	Concede permiso para importar resultados en Security Hub desde un producto integrado.	Escritura	product*		
				securityhub:TargetAccount	
BatchUpdateAutomationRules	Otorga permiso para actualizar una o más reglas de automatización desde Security Hub en función de los nombres de recursos de Amazon (ARNs) y los parámetros de entrada de la regla	Escritura	automation-rule*		
BatchUpdateFindings	Concede permiso para actualizar campos controlados por el cliente para un conjunto seleccionado de hallazgos de Security Hub	Escritura	hub		
			hubv2		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath} securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchUpdateStandardsControlAssociations	Concede permiso para actualizar el estado de habilitación de un lote de controles de seguridad en estándares	Escritura			securityhub:UpdateStandardsControl
ConnectorRegistrationsV2	Otorga permiso para completar el flujo de códigos de autorización OAuth 2.0 en función de los parámetros de entrada	Escritura			
CreateActionTarget	Concede permiso para crear acciones personalizadas en Security Hub.	Escritura	hub		
CreateAggregatorV2	Otorga permiso para crear un AggregatorV2, que configura la agregación de datos en todas las regiones	Escritura			
CreateAutomationRule	Concede permiso para crear una regla de automatización en función de los parámetros de entrada	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAutomationRuleV2	Otorga permiso para crear una regla de automatización V2 en función de los parámetros de entrada	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	Concede permiso para crear una política de configuración para administrar los ajustes de los miembros de la organización en Security Hub	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorV2	Otorga permiso para crear un conector V2 en función de los parámetros de entrada	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	Concede permiso para crear un agregador de búsquedas, que contiene la configuración de agregación de búsquedas entre regiones.	Escritura			
CreateInsight	Concede permiso para crear información en Security Hub. Las observaciones son colecciones de hallazgos relacionados.	Write	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMembers	Concede permiso para crear cuentas de miembros en Security Hub.	Escritura	hub		
CreateTicketV2	Otorga permiso para crear un ticket para un hallazgo de OCSF seleccionado	Escritura	connectorv2		
DeclineInvitations	Concede permiso para rechazar las invitaciones de Security Hub para convertirse en una cuenta de miembro.	Write	hub		
DeleteActionTarget	Concede permiso para eliminar acciones personalizadas en Security Hub.	Escritura	hub		
DeleteAggregatorV2	Otorga permiso para eliminar un AggregatorV2, que configura la agregación de datos en todas las regiones	Escritura	aggregatorv2*		
DeleteAutomationRuleV2	Concede permiso para eliminar una regla de automatización V2 en Security Hub	Escritura	automation-rulev2*		
DeleteConfigurationPolicy	Concede permiso para eliminar una política de configuración existente	Escritura	configuration-policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConnectorV2	Concede permiso para eliminar un conector V2 en Security Hub	Escritura	connectorv2*		
DeleteFindingAggregator	Concede permiso para eliminar un agregador de búsquedas, que desactiva la búsqueda de agregación en todas las regiones.	Escritura	finding-aggregator*		
DeleteInsight	Concede permiso para eliminar información de Security Hub.	Write	hub		
DeleteInvitations	Concede permiso para eliminar invitaciones de Security Hub para convertirse en una cuenta miembro.	Write	hub		
DeleteMembers	Concede permiso para eliminar cuentas de miembros de Security Hub.	Write	hub		
DescribeActionTargets	Concede permiso para recuperar una lista de acciones personalizadas mediante la API.	Read	hub		
DescribeHub	Concede permiso para recuperar información sobre el recurso Hub en su cuenta.	Read	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeOrganizationConfiguration	Concede permiso para describir la configuración de la organización para Security Hub.	Read	hub		
DescribeProducts	Concede permiso para recuperar información sobre las integraciones de productos de Security Hub disponibles.	Lectura	hub		
DescribeProductsV2	Otorga permiso para recuperar información sobre las integraciones de productos de Security Hub V2 disponibles	Lectura	hubv2		
DescribeSecurityHubV2	Otorga permiso para recuperar información sobre el recurso hub V2 de su cuenta	Lectura			
DescribeStandards	Concede permiso para recuperar información acerca de los estándares de Security Hub.	Read	hub		
DescribeStandardsControls	Concede permiso para recuperar información acerca de los controles de estándares de Security Hub.	Read	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableImportFindingsForProduct	Concede permiso para desactivar la importación de resultados para un producto integrado de Security Hub.	Write	hub		
DisableOrganizationAdminAccount	Concede permiso para quitar la cuenta de administrador para su Security Hub de su organización.	Write	hub		organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedAdministrators
DisableSecurityHub	Concede permiso para desactivar Security Hub.	Escritura	hub		
DisableSecurityHubV2	Otorga permiso para deshabilitar Security Hub V2	Escritura			
DisassociateFromAdministratorAccount	Concede permiso a una cuenta miembro de Security Hub para desvincular de la cuenta del administrador asociada.	Write	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateFromMasterAccount	Concede permiso a una cuenta miembro de Security Hub para desvincular de la cuenta maestra asociada.	Write	hub		
DisassociateMembers	Concede permiso para desasociar las cuentas de miembros de Security Hub de la cuenta del administrador asociada	Write	hub		
EnableImportFindingsForProduct	Concede permiso para habilitar la importación de resultados para un producto integrado de Security Hub.	Write	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableOrganizationAdminAccount	Concede permiso para designar una cuenta de administrador de Security Hub para su organización.	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Concede permiso para habilitar Security Hub.	Escritura	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableSecurityHubV2	Otorga permiso para activar Security Hub V2	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults [solo permiso]	Otorga permiso para recuperar datos estadísticos agregados sobre los hallazgos	Lectura	hub hubv2		
GetAdministratorAccount	Concede permiso para recuperar detalles sobre la cuenta de administrador de Security Hub	Lectura	hub		
GetAggregatorV2	Otorga permiso para recuperar los detalles de un AggregatorV2, que configura la agregación de datos en todas las regiones	Lectura	aggregatorv2*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAutomationRuleV2	Otorga permiso para recuperar los detalles de una regla de automatización V2 desde Security Hub en función de la regla Amazon Resource Name (ARN)	Lectura	automation-rulev2*		
GetConfigurationPolicy	Concede permiso para obtener una visión general completa de una política de configuración creada por la cuenta que realiza la llamada	Lectura	configuration-policy*		
GetConfigurationPolicyAssociation	Concede permiso para recuperar información sobre una política de configuración asociada a una cuenta de miembro o unidad organizacional de la organización de la cuenta que realiza la llamada	Lectura			
GetConnectorV2	Otorga permiso para recuperar los detalles de un conector V2 del Security Hub en función del identificador del conector	Lectura	connectorv2*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetControlFindingSummary [solo permiso]	Concede permiso para recuperar una puntuación de seguridad y recuentos de los estados de búsqueda y control para un estándar de seguridad .	Read	hub		
GetEnabledStandards	Concede permiso para recuperar una lista de los estándares habilitados en Security Hub.	Enumeración	hub		
GetFindingAggregator	Concede permiso para recuperar detalles de un agregador de búsquedas, que configura la agregación de búsqueda en todas las regiones.	Lectura	finding-aggregator*		
GetFindingHistory	Concede permiso para recuperar una lista de historial de resultados de Security Hub	Lectura	hub		
GetFindings	Concede permiso para recuperar una lista de hallazgos de Security Hub.	Read	hub		
			hubv2		
GetFreeTrialEndDate [solo permiso]	Concede permiso para recuperar la fecha de finalización de la prueba gratuita de una cuenta de Security Hub	Read	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetFreeTrialUsage [solo permiso]	Concede permiso para recuperar información sobre el uso de Security Hub durante el periodo de prueba gratuito	Read	hub		
GetInsightFindingTrend [solo permiso]	Concede permiso para recuperar una tendencia de búsqueda de conocimiento desde Security Hub con el fin de generar un gráfico	Read	hub		
GetInsightResults	Concede permiso para recuperar los resultados de información de Security Hub.	Read	hub		
GetInsights	Concede permiso para recuperar información de Security Hub.	List	hub		
GetInvitationsCount	Concede permiso para recuperar el recuento de invitaciones para hacerse miembro de Security Hub enviadas a la cuenta.	Read	hub		
GetMasterAccount	Concede permiso para recuperar detalles sobre la cuenta maestra de Security Hub.	Read	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMembers	Concede permiso para recuperar los detalles de las cuentas de miembros de Security Hub.	Lectura	hub		
GetResourcesStatisticsV2	Otorga permiso para recuperar estadísticas agregadas sobre los recursos	Lectura	hubv2		
GetResourcesV2	Otorga permiso para recuperar una lista de recursos	Lectura	hubv2		
GetSecurityControlDefinition	Concede permiso para obtener detalles sobre controles de seguridad específicos identificados por ID	Lectura			securityhub:DescribeStandardsControls
GetUsage [solo permiso]	Concede permiso para recuperar información acerca del uso de cuentas de Security Hub.	Lectura	hub		
InviteMembers	Otorga permiso para invitar a otras AWS cuentas a convertirse en cuentas de miembros de Security Hub	Escritura	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAggregatorsV2	Otorga permiso para recuperar una lista de AggregatorsV2, que configura la agregación de datos en todas las regiones	Enumeración			
ListAutomationRules	Concede permiso para recuperar una lista de reglas de automatización y sus metadatos para la cuenta de llamada de Security Hub	Enumeración			
ListAutomationRulesV2	Otorga permiso para recuperar una lista de reglas de automatización V2 y sus metadatos para la cuenta que realiza la llamada desde Security Hub	Enumeración			
ListConfigurationPolicies	Concede permiso para enumerar los resúmenes de todas las políticas de configuración creadas por la cuenta que realiza la llamada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConfigurationPolicyAssociations	Concede permiso para recuperar información sobre todas las políticas de configuración asociadas a todas las cuentas de miembros y unidades organizativas de la organización de la cuenta que realiza la llamada	Enumeración			
ListConnectorsV2	Otorga permiso para recuperar una lista de conectores V2 y sus metadatos para la cuenta llamante de Security Hub	Enumeración			
ListControlEvaluationSummaries [solo permiso]	Otorga permiso para recuperar una lista de controles de un estándar, incluidos los controles IDs, los estados y los recuentos de búsquedas	Lectura	hub		
ListEnabledProductsForImport	Concede permiso para recuperar los productos integrados de Security Hub que están habilitados actualmente.	Enumeración	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFindingAggregators	Concede permiso para recuperar una lista de agregadores de búsqueda, que contienen la configuración de agregación de búsqueda entre regiones.	Enumeración			
ListInvitations	Concede permiso para recuperar las invitaciones de Security Hub enviadas a la cuenta.	List	hub		
ListMembers	Concede permiso para recuperar detalles sobre las cuentas de miembros de Security Hub asociadas a la cuenta de administrador	List	hub		
ListOrganizationAdminAccounts	Concede permiso para enumerar las cuentas de administrador de Security Hub para su organización.	Enumeración	hub		organizations:DescribeOrganization organizations:ListDelegatedAdministrators

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSecurityControlDefinitions	Concede permiso para recuperar una lista de definiciones de control de seguridad, que contienen detalles de los controles de seguridad de la región actual	Enumeración			
ListStandardsControlAssociations	Concede permiso para enumerar el estado de habilitación de un control de seguridad en estándares	Enumeración			securityhub:DescribeStandardsControls
ListTagsForResource	Concede permiso para mostrar las etiquetas asociadas a un recurso.	Read	automation-rule		
			configuration-policy		
			hub		
SendFindingsEvents [solo permiso]	Otorga permiso para usar una acción personalizada para enviar las conclusiones del Security Hub a Amazon EventBridge	Lectura	hub		
SendInsightEvents [solo permiso]	Otorga permiso para usar una acción personalizada para enviar información sobre Security Hub a Amazon EventBridge	Lectura	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartConfiguration PolicyAssociation	Concede permiso para asociar una política de configuración a una cuenta miembro o unidad organizativa de la organización de la cuenta que realiza la llamada	Escritura	configuration-policy		
StartConfiguration PolicyDisassociation	Concede permiso para eliminar una asociación de políticas de configuración de una cuenta miembro o unidad organizativa de la organización de la cuenta que realiza la llamada	Escritura	configuration-policy		
TagResource	Concede permiso para agregar etiquetas a un recurso de Centro de seguridad	Etiquetado	automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas de un recurso de Security Hub.	Etiquetado	automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UpdateActionTarget	Concede permiso para actualizar acciones personalizadas en Security Hub.	Escritura	hub		
UpdateAggregatorV2	Otorga permiso para actualizar un AggregatorV2, que configura la agregación de datos en todas las regiones	Escritura	aggregatorv2*		
UpdateAutomationRuleV2	Otorga permiso para actualizar una regla de automatización V2 en Security Hub en función del nombre de recurso de Amazon (ARN) de la regla y los parámetros de entrada	Escritura	automation-rulev2*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConfigurationPolicy	Concede permiso para actualizar una política de configuración existente	Escritura	configuration-policy*		
UpdateConnectorV2	Concede permiso para actualizar un conector V2 en Security Hub en función del identificador del conector y los parámetros de entrada	Escritura	connectorv2*		
UpdateFindingAggregator	Concede permiso para actualizar un agregador de búsquedas, que contiene la configuración de agregación de búsquedas entre regiones.	Escritura	finding-aggregator*		
UpdateFindings	Concede permiso para actualizar los resultados de Security Hub.	Write	hub		
UpdateInsight	Concede permiso para actualizar información en Security Hub.	Write	hub		
UpdateOrganizationConfiguration	Concede permiso para actualizar la configuración de la organización para Security Hub.	Escritura	hub		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSecurityControl	Concede permiso para actualizar las propiedades de un control de seguridad específico identificado por ID o ARN	Escritura			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Concede permiso para actualizar la configuración de Security Hub	Write	hub		
UpdateStandardsControl	Concede permiso para actualizar los controles de estándares de Security Hub.	Write	hub		

Tipos de recursos definidos por AWS Security Hub

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
hub	`arn:${Partition}:securityhub:${Region}:${Account}:hub/default`	aws:ResourceTag/${TagKey}
hubv2	`arn:${Partition}:securityhub:${Region}:${Account}:hubv2/${HubV2Id}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
product	arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}	
finding-aggregator	arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}	
aggregatorv2	arn:${Partition}:securityhub:${Region}:${Account}:aggregatorv2/${AggregatorV2Id}	
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	
automation-rulev2	arn:${Partition}:securityhub:${Region}:${Account}:automation-rulev2/${AutomationRuleV2Id}	aws:ResourceTag/${TagKey}
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	
connectorv2	arn:${Partition}:securityhub:${Region}:${Account}:connectorv2/${ConnectorV2Id}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Security Hub

AWS Security Hub define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante acciones en función de pares de clave-valor asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante acciones en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filtra el acceso mediante los campos y valores específicos en la solicitud	Cadena
securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	Filtra el acceso mediante los campos y valores específicos en la solicitud.	Cadena
securityhub:TargetAccount	Filtra el acceso por el AwsAccountId campo especificado en la solicitud	Cadena

Claves de condiciones, recursos y acciones para la respuesta a incidentes AWS de seguridad

AWS La respuesta a incidentes de seguridad (prefijo de servicio:`security-ir`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la respuesta a incidentes de seguridad AWS
- Tipos de recursos definidos por la respuesta a incidentes de AWS seguridad
- Claves de condición para la respuesta a incidentes de AWS seguridad

Acciones definidas por la respuesta a incidentes de seguridad AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetMemberAccountDetails	Otorga permiso para obtener los detalles de las cuentas de los miembros por lotes	Lectura	membership*		
CancelMembership	Otorga permiso para cancelar una membresía	Escritura	membership*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CloseCase	Otorga permiso para cerrar un caso	Escritura	case*		
CreateCase	Otorga permiso para crear un caso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCaseComment	Otorga permiso para crear un comentario de caso	Escritura	case*		
CreateMembership	Otorga permiso para crear una membresía	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:ListDelegatedAdministrators
GetCase	Otorga permiso para obtener una funda	Lectura	case*		
GetCaseAttachmentDownloadUrl	Otorga permiso para obtener la URL de descarga de un archivo adjunto de un caso	Lectura	case*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCaseAttachmentUploadUrl	Otorga permiso para obtener la URL de carga de un archivo adjunto de un caso	Escritura	case*		
GetMembership	Otorga permiso para obtener una membresía	Lectura	membership*		
ListCaseEdits	Otorga permiso para enumerar las ediciones de casos	Lectura	case*		
ListCases	Otorga permiso para enumerar casos	Enumeración			
ListComments	Otorga permiso para enumerar los comentarios de los casos	Lectura	case*		
ListMemberships	Otorga permiso para incluir las membresías	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas adjuntas al recurso especificado	Lectura	case		
			membership		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource		Etiquetado	case		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para agregar etiquetas al recurso especificado		membership		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas del recurso especificado	Etiquetado	case		
			membership		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCase	Otorga permiso para actualizar un caso	Escritura	case*		
UpdateCaseComment	Otorga permiso para actualizar el comentario de un caso	Escritura	case*		
UpdateCaseStatus	Otorga permiso para actualizar el estado de un caso	Escritura	case*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMembership	Otorga permiso para actualizar las membresías	Escritura	membership*		iam:CreateServiceLinkedRole
UpdateResolverType	Otorga permiso para actualizar el tipo de resolución de casos	Escritura	case*		

Tipos de recursos definidos por la respuesta a incidentes de AWS seguridad

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
case	`arn:${Partition}:security-ir:${Region}:${Account}:case/${CaseId}`	aws:ResourceTag/${TagKey}
membership	`arn:${Partition}:security-ir:${Region}:${Account}:membership/${MembershipId}`	aws:ResourceTag/${TagKey}

Claves de condición para la respuesta a incidentes de AWS seguridad

AWS La respuesta a incidentes de seguridad define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para

ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Security Lake

Amazon Security Lake (prefijo de servicio: `securitylake`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Security Lake
- Tipos de recursos definidos por Amazon Security Lake
- Claves de condición de Amazon Security Lake

Acciones definidas por Amazon Security Lake

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAwsLogSource	Concede permiso para habilitar cualquier tipo de origen en cualquier región para cuentas que formen parte de una organización de confianza o cuenta independiente	Escritura	data-lake*		glue:CreateDatabase glue:CreateTable glue:GetDatabase glue:GetTable iam:CreateServiceLinkedRole kms:CreateGrant kms:DescribeKey
CreateCustomLogSource	Concede permiso para agregar un origen personalizado	Escritura	data-lake*		glue:CreateCrawler glue:CreateDatabase glue:CreateTable

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					glue:StartCrawlerSchedule iam:DeleteRolePolicy iam:GetRole iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey kms:GenerateDataKey lakeformation:GrantPermissions lakeformation:Regi

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					sterResource s3:ListBucket s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDataLake	Concede permiso para crear un nuevo lago de datos de seguridad	Escritura	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetD

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListAccounts organizations:ListDelegatedServicesF

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					orAccount s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					sqs:SetQueueAttributes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeExceptionSubscription	Concede permiso para recibir notificaciones instantáneas sobre excepciones. Realiza la suscripción a los temas de SNS para notificaciones de excepciones	Escritura			
CreateDataLakeOrganizationConfiguration	Concede permiso para habilitar automáticamente Amazon Security Lake para las nuevas cuentas de miembros de su organización	Escritura	data-lake*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSubscriber	Concede permiso para crear un suscriptor	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateRole iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy lakeformation:GrantPermissions lakeformation:ListPermissions lakeformation:RegisterResource lakeformation:RevokePermissions

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ram:GetResourceShareAssociations ram:GetResourceShares ram:UpdateResourceShare s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSubscriberNotification	Concede permiso para crear una invocación de webhook para notificar a un cliente cuando haya datos nuevos en el lago de datos	Escritura	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:PassRole s3:GetBucketNotification s3:PutBucketNotification sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAwsLogSource	Concede permiso para deshabilitar cualquier tipo de origen en cualquier región para cuentas que formen parte de una organización de confianza o cuentas independientes	Escritura	data-lake*		
DeleteCustomLogSource	Concede permiso para eliminar un origen personalizado	Escritura	data-lake*		glue:StopCrawlerSchedule
DeleteDataLake	Concede permiso para eliminar un lago de datos de seguridad	Escritura	data-lake*		organizations:DescribeOrganization organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDataLakeExceptionSubscription	Otorga permiso para darse de baja de temas de SNS para notificaciones de excepciones. Elimina las notificaciones de excepciones para el tema de SNS	Escritura			
DeleteDataLakeOrganizationConfiguration	Concede permiso para eliminar la habilitación automática del acceso a Amazon Security Lake para las nuevas cuentas de organización	Escritura	data-lake*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSubscriber	Concede permiso para eliminar al suscriptor especificado	Escritura	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:GetRole iam:ListRolePolicies lakeformation:ListPermissions lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSubscriberNotification	Concede permiso para eliminar una invocación de webhook para notificar a un cliente cuando haya datos nuevos en el lago de datos	Escritura	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:GetRole iam:ListRolePolicies lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl
DeregisterDataLakeDelegatedAdministrator	Otorga permiso para eliminar la cuenta de administrador delegado y deshabilitar Amazon Security Lake como servicio para esta organización	Escritura			organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDataLakeExceptionSubscription	Concede permiso para consultar el protocolo y el punto de conexión que se proporcionaron al suscribirse a temas de SNS para notificaciones de excepciones	Lectura			
GetDataLakeOrganizationConfiguration	Concede permiso para obtener el ajuste de la configuración de la organización para habilitar automáticamente el acceso a Amazon Security Lake para nuevas cuentas de la organización	Lectura	data-lake*		organizations:DescribeOrganization
GetDataLakeSources	Concede permiso para obtener una instantánea estática del lago de datos de seguridad en la región actual. La instantánea incluye las cuentas habilitadas y los orígenes de registros	Lectura	data-lake*		
GetSubscriber	Concede permiso para obtener información sobre un suscriptor que ya se ha creado	Lectura	subscriber*		
ListDataLakeExceptions	Concede permiso para obtener la lista de todos los errores que no se pueden volver a intentar	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDataLakes	Concede permiso para enumerar información sobre los lagos de datos de seguridad	Enumeración			
ListLogSources	Concede permiso para ver las cuentas habilitadas. Concede permiso para ver los orígenes habilitados en las regiones habilitadas	Enumeración			
ListSubscribers	Concede permiso para enumerar todos los suscriptores	Enumeración			
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas del recurso	Enumeración	data-lake		
			subscriber		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterDataLakeDelegatedAdministrator	Concede permiso para designar una cuenta como cuenta de administrador de Amazon Security Lake para la organización	Escritura			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount organizations:RegisterDelegatedAdministrator

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar etiquetas al recurso	Etiquetado	data-lake		
			subscriber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas del recurso	Etiquetado	data-lake		
			subscriber		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDataLake	Concede permiso para actualizar un lago de datos de seguridad	Escritura	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetDataLakeSettings

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount s3:CreateBucket s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes sqs:SetQueueAttributes
UpdateDataLakeExceptionSubscription	Otorga permiso para actualizar las suscripciones a los temas de SNS para notificaciones de excepciones	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSubscriber	Concede permiso para actualizar un suscriptor	Escritura	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:PutRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSubscriberNotification	Concede permiso para actualizar una invocación de webhook para notificar a un cliente cuando haya datos nuevos en el lago de datos	Escritura	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					iam:GetRole iam:PassRole iam:PutRolePolicy s3:CreateBucket s3:GetBucketNotification s3:ListBucket s3:PutBucketNotification s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					s3:PutLifecycleConfiguration sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Tipos de recursos definidos por Amazon Security Lake

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
data-lake	`arn:${Partition}:securitylake:${Region}:${Account}:data-lake/default`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}
subscriber	`arn:${Partition}:securitylake:${Region}:${Account}:subscriber/${SubscriberId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Claves de condición de Amazon Security Lake

Amazon Security Lake define las siguientes claves de condición que se pueden usar en el elemento de `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Server Migration Service

AWS El Servicio de migración de servidores (prefijo de servicio:`sms`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Server Migration Service
- Tipos de recursos definidos por AWS Server Migration Service
- Claves de condición para AWS Server Migration Service

Acciones definidas por AWS Server Migration Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApp	Otorga permiso para crear una configuración de aplicación a la que migrar la aplicación local AWS	Escritura			
CreateReplicationJob	Otorga permiso para crear un trabajo al que migrar un servidor local AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteApp	Concede permiso para eliminar una configuración de aplicación existente	Write			
DeleteAppLaunchConfiguration	Concede permiso para eliminar la configuración de inicio de una aplicación existente	Write			
DeleteAppReplicationConfiguration	Concede permiso para eliminar la configuración de replicación de una aplicación existente	Write			
DeleteAppValidationConfiguration	Concede permiso para eliminar la configuración de validación de una aplicación existente	Escritura			
DeleteReplicationJob	Otorga permiso para eliminar un trabajo existente al que migrar un servidor local AWS	Escritura			
DeleteServerCatalog	Otorga permiso para eliminar la lista completa de servidores locales recopilados en AWS	Escritura			
DisassociateConnector	Concede permiso para desasociar un conector asociado	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GenerateChangeSet	Otorga permiso para generar un ChangSet para la CloudFormation pila de una aplicación	Escritura			
GenerateTemplate	Otorga permiso para generar una CloudFormation plantilla para una aplicación existente	Escritura			
GetApp	Concede permiso para obtener la configuración y los estados de una aplicación existente	Lectura			
GetAppLaunchConfiguration	Concede permiso para obtener la configuración de inicio de una aplicación existente	Read			
GetAppReplicationConfiguration	Concede permiso para obtener la configuración de replicación para una aplicación existente	Read			
GetAppValidationConfiguration	Concede permiso para obtener la configuración de validación de una aplicación existente	Read			
GetAppValidationOutput	Concede permiso para recibir notificaciones enviadas desde el script de validación de aplicaciones.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConnectors	Concede permiso para obtener todos los conectores que se han asociado	Read			
GetMessages [solo permiso]	Otorga permiso para obtener mensajes del Servicio de migración de AWS servidores al conector de migración de servidores	Lectura			
GetReplicationJobs	Otorga permiso para migrar todos los trabajos existentes a los servidores locales AWS	Lectura			
GetReplicationRuns	Concede permiso para obtener todas las ejecuciones de un trabajo existente	Read			
GetServers	Concede permiso para obtener todos los servidores que se han importado	Lectura			
ImportAppCatalog	Otorga permiso para importar el catálogo de aplicaciones desde AWS Application Discovery Service	Escritura			
ImportServerCatalog	Concede permiso para recopilar una lista completa de servidores locales	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
LaunchApp	Otorga permiso para crear y lanzar una CloudFormation pila para una aplicación existente	Escritura			
ListApps	Concede permiso para obtener una lista de resúmenes de las aplicaciones existentes	List			
NotifyAppValidationOutput	Concede permiso para enviar notificaciones para el script de validación de aplicaciones	Write			
PutAppLaunchConfiguration	Concede permiso para crear o actualizar la configuración de lanzamiento de una aplicación existente	Write			
PutAppReplicationConfiguration	Concede permiso para crear o actualizar la configuración de replicación de una aplicación existente	Write			
PutAppValidationConfiguration	Concede permiso para poner la configuración de validación para una aplicación existente	Write			
SendMessage [solo permiso]	Otorga permiso para enviar un mensaje desde el conector de migración de AWS servidores al servicio de migración de servidores	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartAppReplication	Concede permiso para crear e iniciar trabajos de replicación para una aplicación existente	Write			
StartOnDemandAppReplication	Concede permiso para iniciar una ejecución de replicación para una aplicación existente	Write			
StartOnDemandReplicationRun	Concede permiso para iniciar una ejecución de replicación para un trabajo de replicación existente	Write			
StopAppReplication	Concede permiso para detener y eliminar trabajos de replicación para una aplicación existente	Escritura			
TerminateApp	Otorga permiso para terminar la CloudFormation pila de una aplicación existente	Escritura			
UpdateApp	Concede permiso para actualizar una configuración de aplicación existente	Escritura			
UpdateReplicationJob	Otorga permiso para actualizar un trabajo existente y migrarlo a un servidor local AWS	Escritura			

Tipos de recursos definidos por AWS Server Migration Service

AWS El Servicio de migración de servidores no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Server Migration Service, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Server Migration Service

ServerMigrationService no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Serverless Application Repository

AWS Serverless Application Repository (prefijo de servicio`serverlessrepo`:) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Serverless Application Repository
- Tipos de recursos definidos por AWS Serverless Application Repository
- Claves de condición para AWS Serverless Application Repository

Acciones definidas por AWS Serverless Application Repository

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateApplication	Otorga permiso para crear una aplicación y, si lo desea, incluye un archivo AWS SAM para crear la primera versión de la aplicación en la misma llamada	Escritura			
CreateApplicationVersion	Otorga permiso para crear una versión de una aplicación	Escritura	applications*		
CreateCloudFormationChangeSet	Otorga permiso para crear un AWS CloudFormation ChangeSet archivo para la aplicación en cuestión	Escritura	applications*		
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	Otorga permiso para crear una AWS CloudFormation plantilla	Escritura	applications*		
				serverlessrepo:applicationType	
DeleteApplication	Otorga permiso para eliminar la aplicación especificada	Escritura	applications*		
GetApplication	Otorga permiso para obtener la aplicación especificada	Lectura	applications*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				serverlessrepo:applicationType	
GetApplicationPolicy	Otorga permiso para obtener la política de la aplicación especificada	Lectura	applications*		
GetCloudFormationTemplate	Otorga permiso para obtener la AWS CloudFormation plantilla especificada	Lectura	applications*		
ListApplicationDependencies	Otorga permiso para devolver la lista de aplicaciones anidadas en la aplicación contenedora	Enumeración	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	Otorga permiso para enumerar las versiones de la aplicación especificada que pertenecen al solicitante	Enumeración	applications*		
				serverlessrepo:applicationType	
ListApplications	Otorga permiso para enumerar las aplicaciones que pertenecen al solicitante	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutApplicationPolicy	Otorga permiso para poner la política de la aplicación especificada	Escritura	applications*		
SearchApplications	Otorga permiso para obtener todas las aplicaciones autorizadas para este usuario	Lectura		serverlessrepo:applicationType	
UnshareApplication	Otorga permiso para dejar de compartir la aplicación especificada	Escritura	applications*		
UpdateApplication	Otorga permiso para actualizar los metadatos de la aplicación	Escritura	applications*		

Tipos de recursos definidos por AWS Serverless Application Repository

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

Claves de condición para AWS Serverless Application Repository

AWS Serverless Application Repository define las siguientes claves de condición que se pueden usar en `Condition` el elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
serverlessrepo:applicationType	Filtra el acceso por tipo de aplicación	Cadena

Claves de condición, recursos y acciones de AWS Service - Oracle Database@AWS

AWS Servicio: Oracle Database@AWS (prefijo de servicio:odb) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por el servicio: Oracle Database@ AWSAWS
- Tipos de recursos definidos por el AWS servicio: Oracle Database@AWS
- Claves de condición del AWS servicio: Oracle Database@AWS

Acciones definidas por el servicio: Oracle Database@ AWSAWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptMarketplaceRegistration	Concede permiso para registrar el token de Amazon Web Services Marketplace en su cuenta de Amazon Web Services para activar su suscripción a Oracle Database @Amazon Web Services	Escritura			
CreateCloudAutonomousVmCluster	Otorga permiso para crear un nuevo clúster de máquinas virtuales autónomas en la infraestructura de Exadata especificada	Escritura	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudExadataInfrastructure	Otorga permiso para crear una infraestructura de Exadata	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCloudVmCluster	Otorga permiso para crear un clúster de máquinas virtuales en la infraestructura de Exadata especificada	Escritura	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbNode [solo permiso]	Otorga permiso para crear un nodo de base de datos	Escritura	db-node*		
CreateOdbNetwork	Otorga permiso para crear una red ODB	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOdbPeeringConnection	Otorga permiso para crear una conexión de emparejamiento ODB	Escritura	odb-network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundIntegration [solo permiso]	Otorga permiso para crear una integración saliente	Escritura	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		
DeleteCloudAutonomousVmCluster	Otorga permiso para eliminar un clúster de máquinas virtuales autónomas	Escritura	cloud-autonomous-vm-cluster*		
DeleteCloudExadataInfrastructure	Otorga permiso para eliminar una infraestructura de Exadata específica. Antes de utilizar esta operación, asegúrese de eliminar todos los clústeres de máquinas virtuales alojados en esta infraestructura de Exadata	Escritura	cloud-exadata-infrastructure*		
DeleteCloudVmCluster	Otorga permiso para eliminar un clúster de máquinas virtuales específico	Escritura	cloud-vm-cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDbNode [solo permiso]	Otorga permiso para eliminar un nodo de base de datos	Escritura	db-node*		
DeleteOdbNetwork	Otorga permiso para eliminar la red ODB especificada	Escritura	odb-network*		
DeleteOdbPeeringConnection	Otorga permiso para eliminar la conexión de emparejamiento ODB especificada. Al eliminar una conexión de emparejamiento ODB, también se elimina la conexión de emparejamiento de VPC subyacente	Escritura	odb-peering-connection*		
DeleteResourcePolicy [solo permiso]	Concede permiso para eliminar una política de recursos.	Escritura	cloud-exadata-infrastructure*		
			odb-network*		
GetCloudAutonomousVmCluster	Otorga permiso para obtener información sobre un clúster de máquinas virtuales autónomas específico	Lectura	cloud-autonomous-vm-cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCloudExadataInfrastructure	Otorga permiso para obtener información sobre la infraestructura de Exadata especificada	Lectura	cloud-exadata-infrastructure*		
GetCloudExadataInfrastructureUnallocatedResources	Otorga permiso para recuperar información sobre los recursos no asignados en una infraestructura de Cloud Exadata específica	Lectura	cloud-exadata-infrastructure*		
GetCloudVmCluster	Otorga permiso para obtener información sobre el clúster de máquinas virtuales especificado	Lectura	cloud-vm-cluster*		
GetDbNode	Otorga permiso para obtener información sobre el nodo de base de datos especificado	Lectura	cloud-vm-cluster*		
			db-node*		
GetDbServer	Otorga permiso para obtener información sobre el servidor de base de datos especificado	Lectura	cloud-exadata-infrastructure*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOciOnboardingStatus	Otorga permiso para obtener el enlace de activación del arrendamiento y el estado de incorporación de su cuenta de Amazon Web Services	Lectura			
GetOdbNetwork	Otorga permiso para obtener información sobre la red ODB especificada	Lectura	odb-network*		
GetOdbPeeringConnection	Otorga permiso para obtener información sobre la conexión de emparejamiento ODB especificada	Lectura	odb-peering-connection*		
GetResourcePolicy [solo permiso]	Otorga permiso para obtener una política de recursos.	Escritura	cloud-exadata-infrastructure*		
			odb-network*		
InitializeService	Otorga permiso para inicializar el servicio ODB por primera vez en una cuenta	Escritura			
ListAutonomousVirtualMachines	Otorga permiso para enumerar todos los equipos autónomos de un VMs clúster de máquinas virtuales autónomas	Lectura	cloud-autonomous-vm-cluster		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCloudAutonomousVmClusters	Otorga permiso para enumerar todos los clústeres de máquinas virtuales autónomas de una infraestructura específica de Cloud Exadata	Enumeración	cloud-exadata-infrastructure		
ListCloudExadataInfrastructures	Otorga permiso para incluir información sobre las infraestructuras de Exadata que son propiedad de su cuenta de Amazon Web Services	Enumeración			
ListCloudVmClusters	Otorga permiso para incluir información sobre los clústeres de máquinas virtuales que son propiedad de su cuenta de Amazon Web Services o solo los que se encuentran en la infraestructura de Exadata especificada	Enumeración	cloud-exadata-infrastructure		
ListDbNodes	Otorga permiso para incluir información sobre los nodos de base de datos del clúster de máquinas virtuales especificado	Enumeración	cloud-vm-cluster*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDbServers	Otorga permiso para incluir información sobre los servidores de bases de datos que pertenecen a la infraestructura de Exadata especificada	Lectura	cloud-exadata-infrastructure*		
ListDbSystemShapes	Otorga permiso para incluir información sobre las formas que están disponibles para una infraestructura de Exadata	Lectura			
ListGiVersions	Otorga permiso para incluir información sobre las versiones del software Oracle Grid Infrastructure (GI) que están disponibles para un clúster de máquinas virtuales para la forma especificada	Lectura			
ListOdbNetworks	Otorga permiso para incluir información sobre las redes ODB propiedad de su cuenta de Amazon Web Services	Enumeración			
ListOdbPeeringConnections	Otorga permiso para enumerar todas las conexiones de emparejamiento ODB o las asociadas a una red ODB específica	Enumeración	odb-network		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSystemVersions	Otorga permiso para mostrar información sobre las versiones del sistema que están disponibles para un clúster de máquinas virtuales para la GIVersion y la forma especificadas	Lectura			
ListTagsForResource	Otorga permiso para mostrar información sobre las etiquetas aplicadas a este recurso	Lectura	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [solo permiso]	Concede permiso para actualizar una política de recursos	Escritura	cloud-exadata-infrastructure*		
			odb-network*		
RebootDbNode	Otorga permiso para reiniciar el nodo de base de datos especificado en un clúster de máquinas virtuales	Lectura	cloud-vm-cluster*		
			db-node*		
StartDbNode	Otorga permiso para iniciar el nodo de base de datos especificado en un clúster de máquinas virtuales	Lectura	cloud-vm-cluster*		
			db-node*		
StopDbNode	Otorga permiso para detener el nodo de base de datos especificado en un clúster de máquinas virtuales	Lectura	cloud-vm-cluster*		
TagResource	Otorga permiso para aplicar etiquetas al recurso especificado	Etiquetado	cloud-autonomous-vm-cluster		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede permiso para eliminar etiquetas del recurso especificado	Etiquetado	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCloudExadataInfrastructure	Otorga permiso para actualizar las propiedades de un recurso de infraestructura de Exadata	Escritura	cloud-exadata-infrastructure*		
UpdateOdbNetwork	Otorga permiso para actualizar las propiedades de una red ODB específica	Escritura	odb-network*		

Tipos de recursos definidos por el AWS servicio: Oracle Database@AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cloud-autonomous-vm-cluster	`arn:${Partition}:odb:${Region}:${Account}:cloud-autonomous-vm-cluster/${CloudAutonomousVmClusterId}`	aws:ResourceTag/${TagKey}
cloud-exadata-infrastructure	`arn:${Partition}:odb:${Region}:${Account}:cloud-exadata-infrastructure/${CloudExadataInfrastructureId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
cloud-vm-cluster	`arn:${Partition}:odb:${Region}:${Account}:cloud-vm-cluster/${CloudVmClusterId}`	aws:ResourceTag/${TagKey}
db-node	`arn:${Partition}:odb:${Region}:${Account}:db-node/${DbNodeId}`	aws:ResourceTag/${TagKey}
odb-network	`arn:${Partition}:odb:${Region}:${Account}:odb-network/${OdbNetworkId}`	aws:ResourceTag/${TagKey}
odb-peering-connection	`arn:${Partition}:odb:${Region}:${Account}:odb-peering-connection/${OdbPeeringConnectionId}`	aws:ResourceTag/${TagKey}

Claves de condición del AWS servicio: Oracle Database@AWS

AWS Servicio: Oracle Database@AWS define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Service Catalog

AWS Service Catalog (prefijo de servicio:`servicecatalog`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Service Catalog
- Tipos de recursos definidos por AWS Service Catalog
- Claves de condición para AWS Service Catalog

Acciones definidas por AWS Service Catalog

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptPortfolioShare	Otorga permiso para aceptar una cartera que se ha compartido con usted	Write	Portfolio*		
AssociateAttributeGroup	Concede el permiso para asociar un grupo de atributos a una aplicación	Write	Application*		
			AttributeGroup*		
AssociateBudgetWithResource	Otorga permiso para asociar un presupuesto a un recurso	Write			
AssociatePrincipalWithPortfolio	Otorga permiso para asociar una entidad principal de IAM con una cartera, lo que da acceso al principal especificado a los productos que estén asociados a la cartera especificada	Write	Portfolio*		
AssociateProductWithPortfolio	Otorga permiso para asociar un producto a una cartera	Write			
AssociateResource	Concede el permiso para asociar un recurso con una aplicación	Write	Application*		cloudformation:DescribeStacks resource-groups:Cr

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					eateGroup resource-groups:GetGroup resource-groups:Tag
				servicecatalog:ResourceType servicecatalog:Resource	
AssociateServiceActionWithProvisioningArtifact	Otorga permiso para asociar una acción con un artefacto de aprovisionamiento	Escritura	Product*		
AssociateTagOptionWithResource	Otorga permiso para asociar lo especificado TagOption a la cartera o producto especificado	Escritura	Portfolio		
			Product		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchAssociateServiceActionWithProvisioningArtifact	Otorga permiso para asociar varias acciones de autoservicio con artefactos de aprovisionamiento	Write			
BatchDisassociateServiceActionFromProvisioningArtifact	Otorga permiso para disociar un lote de acciones de autoservicio del artefacto de aprovisionamiento especificado	Write			
CopyProduct	Otorga permiso para copiar el producto de origen especificado en el producto de destino especificado o un nuevo producto	Write			
CreateApplication	Concede permiso para crear una aplicación.	Write	Application*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAttributeGroup	Concede el permiso para crear un grupo de atributos	Write	AttributeGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConstraint	Otorga permiso para crear una restricción en un producto y cartera asociados	Write	Product*		
CreatePortfolio	Otorga permiso para crear una cartera	Escritura	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortfolioShare	Otorga permiso para compartir una cartera de la que eres propietario con otra persona Cuenta de AWS	Administración de permisos	Portfolio*		
CreateProduct	Otorga permiso para crear un producto y el primer artefacto de aprovisionamiento de ese producto	Write	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateProvisionedProductPlan	Otorga permiso para agregar un nuevo plan de producto aprovisionado	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
CreateProvisioningArtifact	Otorga permiso para agregar un nuevo artefacto de aprovisionamiento a un producto existente	Write	Product*		
CreateServiceAction	Otorga permiso para crear una acción de autoservicio	Escritura			
CreateTagOption	Otorga permiso para crear un TagOption	Escritura			
DeleteApplication	Concede el permiso para eliminar una aplicación si se han quitado todas las asociaciones de la aplicación	Write	Application*		
DeleteAttributeGroup	Concede el permiso para eliminar un grupo de atributos si se han quitado todas las asociaciones del grupo de atributos	Write	AttributeGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConstraint	Otorga permiso para quitar y eliminar una restricción existente de un producto y cartera asociados	Write			
DeletePortfolio	Otorga permiso para eliminar una cartera si todas las asociaciones y usos compartidos se han quitado de la cartera	Escritura	Portfolio*		
DeletePortfolioShare	Otorga permiso para dejar de compartir una cartera de la que eres propietario y con la que la Cuenta de AWS compartiste anteriormente	Administración de permisos	Portfolio*		
DeleteProduct	Otorga permiso para eliminar un producto si se han eliminado todas las asociaciones del producto	Write	Product*		
DeleteProvisionedProductPlan	Otorga permiso para eliminar un plan de producto aprovisionado	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteProvisioningArtifact	Otorga permiso para eliminar un artefacto de aprovisionamiento de un producto	Escritura	Product*		
DeleteResourcePolicy [solo permiso]	Concede permiso para eliminar una política basada en recursos para el recurso especificado	Escritura	Application		
			AttributeGroup		
DeleteServiceAction	Otorga permiso para eliminar una acción de autoservicio	Escritura			
DeleteTagOption	Otorga permiso para eliminar lo especificado TagOption	Escritura			
DescribeConstraint	Otorga permiso para describir una restricción	Read			
DescribeCopyProductStatus	Otorga permiso para obtener el estado de la operación del producto de copia especificada	Read			
DescribePortfolio	Otorga permiso para describir una cartera	Read	Portfolio*		
DescribePortfolioShareStatus	Otorga permiso para obtener el estado de la operación de participación de la cartera especificada	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePortfolioShares	Otorga permiso para ver un resumen de cada una de las acciones de cartera que se crearon para la cartera especificada	List	Portfolio*		
DescribeProduct	Otorga permiso para describir un producto como usuario final	Read	Product*		
DescribeProductAsAdmin	Otorga permiso para describir un producto como administrador	Read	Product*		
DescribeProductView	Otorga permiso para describir un producto como usuario final	Read			
DescribeProvisionedProduct	Otorga permiso para describir un producto aprovisionado	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeProvisionedProductPlan	Otorga permiso para describir un plan de producto aprovisionado	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisioningArtifact	Otorga permiso para describir un artefacto de aprovisionamiento	Read	Product*		
DescribeProvisioningParameters	Otorga permiso para describir los parámetros que debe especificar para aprovisionar correctamente un artefacto de aprovisionamiento especificado	Read	Product*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeRecord	Otorga permiso para describir un registro y enumera las salidas	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeServiceAction	Otorga permiso para describir una acción de autoservicio	Read			
DescribeServiceActionExecutionParameters	Otorga permiso para obtener los parámetros predeterminados si ejecutó la acción de servicio especificada en el producto aprovisionado especificado	Lectura		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeTagOption	Otorga permiso para obtener información sobre lo especificado TagOption	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableAWSOrganizationsAccess	Otorga permiso para deshabilitar el intercambio de portafolios a través de la función AWS Organizations	Escritura			
DisassociateAttributeGroup	Concede el permiso para desasociar un grupo de atributos de una aplicación	Write	Application* AttributeGroup*		
DisassociateBudgetFromResource	Otorga permiso para disociar un presupuesto de un recurso	Write			
DisassociatePrincipalFromPortfolio	Otorga permiso para disociar una entidad principal de IAM de una cartera	Write	Portfolio*		
DisassociateProductFromPortfolio	Otorga permiso para disociar un producto de una cartera	Write			
DisassociateResource	Concede el permiso para desasociar un recurso de una aplicación	Write	Application*		resource-groups:DeleteGroup

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				servicecatalog:ResourceType servicecatalog:Resource	
DisassociateServiceActionFromProvisioningArtifact	Otorga permiso para eliminar la asociación de una acción de autoservicio especificada del artefacto de aprovisionamiento especificado	Escritura	Product*		
DisassociateTagOptionFromResource	Otorga permiso para desasociar lo especificado TagOption del recurso especificado	Escritura	Portfolio		
			Product		
EnableAWSOrganizationsAccess	Otorga permiso para habilitar la función de compartir portafolios a través de AWS Organizations	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExecuteProvisionedProductPlan	Otorga permiso para ejecutar un plan de producto aprovisionado	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ExecuteProvisionedProductServiceAction	Otorga permiso para ejecutar un plan de producto aprovisionado	Escritura		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
GetAWSOrganizationsAccessStatus	Otorga permiso para obtener el estado de acceso a la función de compartir portafolios de AWS la organización	Lectura			
GetApplication	Concede el permiso para obtener una aplicación	Read	Application*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAssociatedResource	Otorga permiso para obtener información sobre un recurso asociado a una aplicación	Read	Application*		
				servicecatalog:ResourceType servicecatalog:Resource	
GetAttributeGroup	Concede el permiso para obtener un grupo de atributos	Lectura	AttributeGroup*		
GetConfiguration	Otorga permiso para leer AppRegistry las configuraciones	Lectura			
GetProvisionedProductOutputs	Otorga permiso para obtener la salida del producto aprovisionado con el identificador del producto aprovisionado o el nombre	Lectura			
GetResourcePolicy [solo permiso]	Concede permiso para obtener una política basada en recursos para el recurso especificado	Lectura	Application		
			AttributeGroup		
ImportAsProvisionedProduct	Concede el permiso para importar un recurso a un producto aprovisionado	Write	Product*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAcceptedPortfolioShares	Otorga permiso para enumerar las carteras que se han compartido con usted y que ha aceptado	Enumeración			
ListApplications	Otorga permiso para enumerar sus aplicaciones	Enumeración			
ListAssociatedAttributeGroups	Concede el permiso para enumerar los grupos de atributos asociados a una aplicación	List	Application*		
ListAssociatedResources	Concede el permiso para enumerar los recursos asociados a una aplicación	Enumeración	Application*		
ListAttributeGroups	Otorga permiso para enumerar sus grupos de atributos	Enumeración			
ListAttributeGroupsForApplication	Otorga permiso para enumerar los grupos de atributos asociados a una aplicación específica	Enumeración	Application*		
ListBudgetsForResource	Otorga permiso para enumerar todos los presupuestos asociados a un recurso	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListConstraintsForPortfolio	Otorga permiso para enumerar las restricciones asociadas a una cartera determinada	List			
ListLaunchPaths	Otorga permiso para enumerar las diferentes formas de lanzar un producto determinado como usuario final	List	Product*		
ListOrganizationPortfolioAccess	Otorga permiso para enumerar los nodos de la organización que tienen acceso a la cartera especificada	Enumeración			
ListPortfolioAccess	Otorga permiso para enumerar las AWS cuentas con las que ha compartido una cartera determinada	Enumeración	Portfolio*		
ListPortfolios	Otorga permiso para publicar las carteras en su cuenta	List			
ListPortfoliosForProduct	Otorga permiso para enumerar las carteras asociadas a un producto determinado	List	Product*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPrincipalsForPortfolio	Otorga permiso para enumerar los principales de IAM asociados a una cartera determinada	List	Portfolio*		
ListProvisionedProductPlans	Otorga permiso para publicar los planes de productos aprovisionados	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListProvisioningArtifacts	Otorga permiso para enumerar los artefactos de aprovisionamiento asociados a un producto determinado	List	Product*		
ListProvisioningArtifactsForServiceAction	Otorga permiso para enumerar todos los artefactos de aprovisionamiento para la acción de autoservicio especificada	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRecordHistory	Otorga permiso para mostrar todos los registros en su cuenta o todos los registros relacionados con un determinado producto aprovisionado	Enumeración		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListResourcesForTagOption	Otorga permiso para enumerar los recursos asociados a la información especificada TagOption	Enumeración			
ListServiceActions	Otorga permiso para enumerar todas las acciones de autoservicio	List			
ListServiceActionsForProvisioningArtifact	Otorga permiso para enumerar todas las acciones de servicio asociadas al artefacto de aprovisionamiento especificado en su cuenta	List	Product*		
				servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListStackInstancesForProvisionedProduct	Otorga permiso para enumerar la cuenta, la región y el estado de cada instancia de pila asociada a un producto aprovisionado de tipo CFN_STACKSET	Enumeración		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListTagOptions	Otorga permiso para enumerar los especificados TagOptions o todos TagOptions	Enumeración			
ListTagsForResource	Concede el permiso para enumerar las etiquetas de un recurso de información de catálogo de servicios	Lectura	Application		
			AttributeGroup		
NotifyProvisionProductEngineWorkflowResult	Concede permiso para notificar el resultado de la ejecución del motor de aprovisionamiento	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
NotifyTerminateProvisionedProductEngineWorkflowResult	Concede permiso para notificar el resultado de la ejecución del motor de finalización	Escritura			
NotifyUpdateProvisionedProductEngineWorkflowResult	Concede permiso para notificar el resultado de la ejecución del motor de actualización	Escritura			
ProvisionProduct	Otorga permiso para aprovisionar un producto con un artefacto de aprovisionamiento especificado y parámetros de lanzamiento	Escritura	Product*		
PutConfiguration	Otorga permiso para asignar AppRegistry configuraciones	Escritura			
PutResourcePolicy [solo permiso]	Concede permiso para agregar una política basada en recursos para el recurso especificado	Escritura	Application		
			AttributeGroup		
RejectPortfolioShare	Otorga permiso para rechazar una cartera que se haya compartido con usted y que haya aceptado previamente	Write	Portfolio*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ScanProvisionedProducts	Otorga permiso para publicar todos los productos aprovisionados en su cuenta	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SearchProducts	Otorga permiso para publicar los productos disponibles para usted como usuario final	List			
SearchProductsAsAdmin	Otorga permiso para enumerar todos los productos de su cuenta o todos los productos asociados a una determinada cartera	List			
SearchProvisionedProducts	Otorga permiso para publicar todos los productos aprovisionados en su cuenta	Enumeración		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SyncResource	Otorga permiso para sincronizar un recurso con su estado actual en AppRegistry	Escritura			cloudformation:UpdateStack
TagResource	Concede el permiso para etiquetar un recurso de Service Catalog AppRegistry	Etiquetado	Application		
			Attribute Group		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateProvisionedProduct	Otorga permiso para finalizar un producto aprovisionado existente	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UntagResource	Concede el permiso para quitar una etiqueta de un recurso de Service Catalog AppRegistry	Etiquetado	Application		
			Attribute Group		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateApplication	Concede el permiso para actualizar los atributos de una aplicación existente	Write	Application*		iam:CreateServiceLinkedRole
UpdateAttributeGroup	Concede el permiso para actualizar los atributos de un grupo de atributos existente	Write	AttributeGroup*		
UpdateConstraint	Otorga permiso para actualizar los campos de metadatos de una restricción existente	Escritura			
UpdatePortfolio	Otorga permiso para actualizar los campos, and/or etiquetas de metadatos de una cartera existente	Escritura	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortfolioShare	Otorga permiso para habilitar o desactivar el uso compartido de recursos para un recurso compartido de cartera existente	Administración de permisos	Portfolio*		
UpdateProduct	Otorga permiso para actualizar los campos y and/or etiquetas de metadatos de un producto existente	Escritura	Product*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProvisionedProduct	Otorga permiso para actualizar un producto aprovisionado existente	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UpdateProvisionedProductProperties	Otorga permiso para actualizar las propiedades de un producto aprovisionado existente	Write			
UpdateProvisioningArtifact	Otorga permiso para actualizar los campos de metadatos de un artefacto de aprovisionamiento existente	Write	Product*		
UpdateServiceAction	Otorga permiso para actualizar una acción de autoservicio	Escritura			
UpdateTagOption	Otorga permiso para actualizar lo especificado TagOption	Escritura			

Tipos de recursos definidos por AWS Service Catalog

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Application	`arn:${Partition}:servicecatalog:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
Attribute Group	`arn:${Partition}:servicecatalog:${Region}:${Account}:/attribute-groups/${AttributeGroupId}`	aws:ResourceTag/${TagKey}
Portfolio	`arn:${Partition}:catalog:${Region}:${Account}:portfolio/${PortfolioId}`	aws:ResourceTag/${TagKey}
Product	`arn:${Partition}:catalog:${Region}:${Account}:product/${ProductId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Service Catalog

AWS Service Catalog define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

> **Note**
>
> Para acceder a ejemplos de políticas que muestran cómo pueden utilizarse estas claves de condición en una política de IAM, consulte Ejemplos de políticas para administrar productos aprovisionados en la Guía del administrador de Service Catalog.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
servicecatalog:Resource	Filtra el acceso controlando qué valor se puede especificar como parámetro de recurso en una API de recursos AppRegistry asociada	Cadena
servicecatalog:ResourceType	Filtra el acceso controlando qué valor se puede especificar como ResourceType parámetro en una API de recursos AppRegistry asociada	Cadena
servicecatalog:accountLevel	Filtra el acceso mediante usuarios para ver y realizar acciones en recursos creados por cualquier persona en la cuenta.	Cadena
servicecatalog:roleLevel	Filtra el acceso mediante usuarios para ver y realizar acciones en recursos creados por ellos o por cualquier persona federada en la misma función que ellos.	Cadena
servicecatalog:userLevel	Filtra el acceso mediante usuarios para ver y realizar acciones solo en recursos que ellos han creado.	Cadena

Acciones, recursos y claves de condición para AWS service providing managed private networks

AWS El servicio que proporciona redes privadas gestionadas (prefijo de servicio:`private-networks`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS service providing managed private networks
- Tipos de recursos definidos por AWS service providing managed private networks
- Claves de condición para AWS service providing managed private networks

Acciones definidas por AWS service providing managed private networks

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcknowledgeOrderReceipt	Concede permiso para confirmar que se ha recibido un pedido	Escritura	order*		
ActivateDeviceIdentifier	Concede permiso para activar un identificador de dispositivo	Escritura	device-identifier*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ActivateNetworkSite	Concede permiso para activar un sitio de red	Escritura	network-site*		
			order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ConfigureAccessPoint	Concede permiso para configurar un punto de acceso	Escritura	network-resource*		
CreateNetwork	Concede permiso para crear una red	Escritura	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkSite	Concede permiso para crear un sitio de red	Escritura	network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateDeviceIdentifier	Concede permiso para desactivar un identificador de dispositivo	Escritura	device-identifier*		
DeleteNetwork	Concede permiso para eliminar una red	Escritura	network*		
DeleteNetworkSite	Concede permiso para eliminar un sitio de red	Escritura	network-site*		
GetDeviceIdentifier	Concede permiso para obtener un identificador de dispositivos	Lectura	device-identifier*		
				aws:ResourceTag/${TagKey}	
GetNetwork	Otorga permiso para obtener una red	Lectura	network*		
				aws:ResourceTag/${TagKey}	
GetNetworkResource	Concede permiso para obtener un recurso de red	Lectura	network-resource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetNetworkSite	Concede permiso para obtener un sitio de red	Lectura	network-site*		
				aws:ResourceTag/${TagKey}	
GetOrder	Concede permiso para obtener un pedido de red	Lectura	order*		
				aws:ResourceTag/${TagKey}	
ListDeviceIdentifiers	Concede permiso para enumerar identificadores de dispositivos	Enumeración	network*		
ListNetworkResources	Concede permiso para enumerar recursos de red	Enumeración	network*		
ListNetworkSites	Concede permiso para enumerar sitios de red	Enumeración	network*		
ListNetworks	Concede permiso para enumerar redes	Enumeración			
ListOrders	Concede permiso para enumerar pedidos de red	Enumeración	network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para devolver una lista de etiquetas de un recurso	Enumeración			
Ping	Otorga permiso para comprobar el estado del servicio	Lectura			
StartNetworkResourceUpdate	Concede permiso para iniciar una actualización en el recurso de red especificado	Escritura	network-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Otorga permiso para agregar etiquetas al recurso especificado	Etiquetado	device-identifier		
			network		
			network-resource		
			network-site		
			order		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar etiquetas del recurso especificado	Etiquetado	device-identifier		
			network		
			network-resource		
			network-site		
			order		
				aws:TagKeys	
UpdateNetworkSite	Concede permiso para actualizar un sitio de red	Escritura	network-site*		
UpdateNetworkSitePlan	Concede permiso para actualizar un plan en un sitio de red	Escritura	network-site*		

Tipos de recursos definidos por AWS service providing managed private networks

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones

identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
network	`arn:${Partition}:private-networks:${Region}:${Account}:network/${NetworkName}`	aws:ResourceTag/${TagKey}
network-site	`arn:${Partition}:private-networks:${Region}:${Account}:network-site/${NetworkName}/${NetworkSiteName}`	aws:ResourceTag/${TagKey}
network-resource	`arn:${Partition}:private-networks:${Region}:${Account}:network-resource/${NetworkName}/${ResourceId}`	aws:ResourceTag/${TagKey}
order	`arn:${Partition}:private-networks:${Region}:${Account}:order/${NetworkName}/${OrderId}`	aws:ResourceTag/${TagKey}
device-identifier	`arn:${Partition}:private-networks:${Region}:${Account}:device-identifier/${NetworkName}/${DeviceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS service providing managed private networks

AWS El servicio que proporciona redes privadas gestionadas define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante la comprobación de la presencia de pares de clave-valor de etiquetas en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la comprobación de los pares de clave-valor de las etiquetas adjuntas al recurso	Cadena
aws:TagKeys	Filtra el acceso según la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para Service Quotas

Service Quotas (prefijo de servicio: `servicequotas`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicas del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Service Quotas
- Tipos de recursos definidos por Service Quotas
- Claves de condición para Service Quotas

Acciones definidas por Service Quotas

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateServiceQuotaTemplate	Da permiso para asociar la plantilla de Service Quotas a su organización	Escritura			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
CreateSupportCase	Concede permiso para enviar una solicitud para crear un caso de soporte para una solicitud de aumento de cuota existente	Escritura			
DeleteServiceQuotaIncreaseRequestFromTemplate	Da permiso para eliminar la cuota de servicio especificada de la plantilla de cuota de servicio	Write			organizations:DescribeOrganization
DisassociateServiceQuotaTemplate	Da permiso para desasociar la plantilla de Service Quotas de su organización	Escritura			organizations:DescribeOrganization
GetAWSDefaultServiceQuota	Otorga permiso para devolver los detalles de la cuota de servicio especificada, incluido el valor AWS predeterminado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAssociationForServiceQuotaTemplate	Otorga permiso para recuperar el ServiceQuotaTemplateAssociationStatus valor, que indica si la plantilla Service Quotas está asociada a una organización	Lectura			organizations:DescribeOrganization
GetRequestedServiceQuotaChange	Da permiso para recuperar los detalles de una solicitud de aumento de cuota de servicio determinada	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceQuota	Da permiso para devolver los detalles de la cuota de servicio especificada, incluido el valor aplicado	Read			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					route53:GetAccountLimit
GetServiceQuotaIncreaseRequestFromTemplate	Da permiso para recuperar los detalles de una solicitud de aumento de cuota de servicio de la plantilla de cuota de servicio	Lectura			organizations:DescribeOrganization
ListAWSDefaultServiceQuotas	Otorga permiso para enumerar todas las cuotas de servicio predeterminadas para el AWS servicio especificado	Lectura			
ListRequestedServiceQuotaChangeHistory	Da permiso para solicitar una lista de los cambios de las cuotas de un servicio	Read			
ListRequestedServiceQuotaChangeHistoryByQuota	Da permiso para solicitar una lista de los cambios a cuotas de servicio específicas	Read			
ListServiceQuotaIncreaseRequestsInTemplate	Da permiso para devolver una lista de las solicitudes de aumento de cuota de servicio de la plantilla de cuota de servicio	Lectura			organizations:DescribeOrganization

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServiceQuotas	Otorga permiso para enumerar todas las cuotas de AWS servicio del servicio especificado, en esa cuenta o región	Lectura			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					route53:GetAccountLimit
ListServices	Otorga permiso para incluir los AWS servicios disponibles en Service Quotas	Lectura			
ListTagsForResource	Concede el permiso para ver las etiquetas existentes en un recurso SQ.	Lectura			
PutServiceQuotaIncreaseRequestIntoTemplate	Da permiso para definir y agregar una cuota a la plantilla de cuota de servicio	Write	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	Da permiso para enviar la solicitud de un aumento de cuota de servicio	Write	quota		
				servicequotas:service	
TagResource	Concede el permiso para asociar un conjunto de etiquetas a un recurso SQ existente.	Etiquetado		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Concede el permiso para quitar un conjunto de etiquetas de un recurso SQ, donde las etiquetas que se van a quitar coinciden con un conjunto de claves de etiqueta suministradas por el cliente.	Etiquetado		aws:TagKeys	

Tipos de recursos definidos por Service Quotas

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Claves de condición para Service Quotas

Service Quotas define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString
servicequotas:service	Filtra el acceso por el AWS servicio especificado	Cadena

Claves de condición, recursos y acciones de Amazon SES

Amazon SES (prefijo de servicio: `ses`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon SES
- Tipos de recursos definidos por Amazon SES
- Claves de condición de Amazon SES

Acciones definidas por Amazon SES

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CloneReceiptRuleSet	Otorga permiso para crear un conjunto de reglas de recepción mediante la clonación de uno existente	Write		ses:ApiVersion	
CreateConfigurationSet	Otorga permiso para crear un nuevo conjunto de configuración	Write		ses:ApiVersion	
CreateConfigurationSetEventDestination	Concede permiso para crear un destino para eventos de conjunto de configuración	Write		ses:ApiVersion	
CreateConfigurationSetTrackingOptions	Otorga permiso para crear una asociación entre un conjunto de configuración y un dominio personalizado para el seguimiento de eventos abiertos y de clic	Write		ses:ApiVersion	
CreateCustomVerificationEmailTemplate	Concede permiso para crear una nueva plantilla de email de verificación personalizada	Write		ses:ApiVersion	
CreateReceiptFilter	Otorga permiso para crear un nuevo filtro de direcciones IP	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateReceiptRule	Otorga permiso para crear una regla de recepción	Write		ses:ApiVersion	
CreateReceiptRuleSet	Otorga permiso para crear un conjunto de reglas de recepción vacío	Write		ses:ApiVersion	
CreateTemplate	Otorga permiso para crear una plantilla de email	Write		ses:ApiVersion	
DeleteConfigurationSet	Concede permiso para eliminar un conjunto de configuración existente	Write		ses:ApiVersion	
DeleteConfigurationSetEventDestination	Concede permiso para eliminar un destino de evento	Write		ses:ApiVersion	
DeleteConfigurationSetTrackingOptions	Otorga permiso para eliminar una asociación entre un conjunto de configuración y un dominio personalizado para el seguimiento de eventos abiertos y de clic	Write		ses:ApiVersion	
DeleteCustomVerificationEmailTemplate	Concede permiso para eliminar una plantilla de email de verificación personalizada existente	Write		ses:ApiVersion	
DeleteIdentity	Otorga permiso para eliminar la identidad especificada	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIdentityPolicy	Concede permiso para eliminar la política de autorización de envío especificada para la identidad dada (una dirección de email o un dominio)	Permissions management		ses:ApiVersion	
DeleteReceiptFilter	Otorga permiso para eliminar el filtro de direcciones IP especificado	Write		ses:ApiVersion	
DeleteReceiptRule	Otorga permiso para eliminar la regla de recepción especificada	Write		ses:ApiVersion	
DeleteReceiptRuleSet	Otorga permiso para eliminar el conjunto de reglas de recepción especificado y todas las reglas de recepción que contiene	Write		ses:ApiVersion	
DeleteTemplate	Otorga permiso para eliminar una plantilla de email	Write		ses:ApiVersion	
DeleteVerifiedEmailAddress	Otorga permiso para eliminar la dirección de email especificada de la lista de direcciones verificadas	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeActiveReceiptRuleSet	Otorga permiso para devolver los metadatos y las reglas de recepción para el conjunto de reglas de recepción que está activo actualmente	Read		ses:ApiVersion	
DescribeConfigurationSet	Otorga permiso para devolver los detalles del conjunto de configuración especificado	Read		ses:ApiVersion	
DescribeReceiptRule	Otorga permiso para devolver los detalles de la regla de recepción especificada	Read		ses:ApiVersion	
DescribeReceiptRuleSet	Otorga permiso para devolver los detalles del conjunto de reglas de recepción especificado	Read		ses:ApiVersion	
GetAccountSendingEnabled	Otorga permiso para devolver el estado de envío de email de su cuenta	Read		ses:ApiVersion	
GetCustomVerificationEmailTemplate	Concede permiso para devolver la plantilla personalizada de verificación de email para el nombre de plantilla especificado	Read		ses:ApiVersion	
GetIdentityDkimAttributes	Otorga permiso para devolver el estado actual de la firma Easy DKIM para una entidad	Lectura		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIdentityMailFromDomainAttributes	Otorga permiso para devolver los atributos MAIL FROM personalizados para una lista de identidades (direcciones de correo electrónico, and/or dominios)	Lectura		ses:ApiVersion	
GetIdentityNotificationAttributes	Otorga permiso para devolver una estructura que describe los atributos de las notificaciones de identidad para una lista de identidades verificadas (direcciones de correo electrónico, and/or dominios),	Lectura		ses:ApiVersion	
GetIdentityPolicies	Concede permiso para devolver las políticas de autorización de envío solicitadas para la identidad dada (una dirección de email o un dominio)	Read		ses:ApiVersion	
GetIdentityVerificationAttributes	Otorga permiso para devolver el estado de verificación y (para identidades de dominio) el token de verificación de una lista de identidades	Read		ses:ApiVersion	
GetSendQuota	Otorga permiso para devolver los límites de envío actuales del usuario	Read		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSendStatistics	Otorga permiso para devolver las estadísticas de envío del usuario	Read		ses:ApiVersion	
GetTemplate	Otorga permiso para devolver el objeto de plantilla, que incluye la línea de asunto, parte en HTML y parte de texto, para la plantilla especificada	Read		ses:ApiVersion	
ListConfigurationSets	Concede permiso para enumerar todos los conjuntos de configuración de su cuenta	List		ses:ApiVersion	
ListCustomVerificationEmailTemplates	Concede permiso para enumerar todas las plantillas de email de verificación personalizadas existentes para su cuenta	List		ses:ApiVersion	
ListIdentities	Otorga permiso para enumerar las identidades de email de su cuenta	List		ses:ApiVersion	
ListIdentityPolicies	Concede permiso para enumerar todas las plantillas de email de su cuenta	List		ses:ApiVersion	
ListReceiptFilters	Otorga permiso para mostrar los filtros de dirección IP asociados a su cuenta	Read		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListReceiptRuleSets	Otorga permiso para mostrar los conjuntos de reglas de recepción que existen en su cuenta	Read		ses:ApiVersion	
ListTemplates	Otorga permiso para mostrar las plantillas de email presentes en su cuenta	List		ses:ApiVersion	
ListVerifiedEmailAddresses	Otorga permiso para mostrar todas las direcciones de email que se han verificado en su cuenta	Read		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Otorga permiso para agregar o actualizar las opciones de entrega de un conjunto de configuración	Write		ses:ApiVersion	
PutIdentityPolicy	Otorga permiso para agregar o actualizar una directiva de autorización de envío para la identidad especificada (una dirección de email o dominio)	Permissions management		ses:ApiVersion	
ReorderReceiptRuleSet	Otorga permiso para volver a ordenar las reglas de recepción dentro de un conjunto de reglas de recepción	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendBounce	Otorga permiso para generar y enviar un mensaje de rebote al remitente de un email que recibió a través de Amazon SES	Write	identity*		
				ses:ApiVersion ses:FromAddress	
SendBulkTemplatedEmail	Concede permiso para redactar un mensaje de email para varios destinos	Write	identity*		
			template*		
			configuration-set		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendCustomVerificationEmail	Otorga permiso para agregar una dirección de email a la lista de identidades e intenta verificarla para su cuenta	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	Concede permiso para enviar un mensaje de correo electrónico	Write	identity*		
			configuration-set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	Otorga permiso para enviar un mensaje de email, con el encabezado y el contenido especificados por el cliente	Write	identity* configuration-set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	Otorga permiso para redactar un mensaje de email mediante una plantilla de email	Write	identity*		
			template*		
			configuration-set		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	Otorga permiso para establecer el conjunto de reglas de recepción especificado como conjunto de reglas de recepción activo	Write		ses:ApiVersion	
SetIdentityDkimEnabled	Otorga permiso para habilitar o desactivar la firma Easy DKIM del email enviado desde una identidad	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetIdentityFeedbackForwardingEnabled	Otorga permiso para habilitar o desactivar si Amazon SES reenvía notificaciones de rebote y quejas para una identidad (una dirección de email o un dominio)	Write		ses:ApiVersion	
SetIdentityHeadersInNotificationsEnabled	Otorga permiso para establecer si Amazon SES incluye los encabezados de email originales en las notificaciones de Amazon Simple Notification Service (Amazon SNS) de un tipo especificado para una identidad determinada (una dirección de email o un dominio)	Write		ses:ApiVersion	
SetIdentityMailFromDomain	Otorga permiso para habilitar o desactivar la configuración del dominio MAIL FROM personalizada para una identidad verificada	Write		ses:ApiVersion	
SetIdentityNotificationTopic	Otorga permiso para establecer un tema de Amazon Simple Notification Service (Amazon SNS) a fin de utilizarlo al entregar notificaciones para una identidad verificada	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetReceiptRulePosition	Otorga permiso para establecer la posición de la regla de recepción especificada en el conjunto de reglas de recepción	Write		ses:ApiVersion	
TestRenderTemplate	Otorga permiso para crear una vista previa del contenido MIME de un email cuando se proporciona con una plantilla y un conjunto de datos de sustitución	Write		ses:ApiVersion	
UpdateAccountSendingEnabled	Otorga permiso para habilitar o desactivar el envío de email para su cuenta	Write		ses:ApiVersion	
UpdateConfigurationSetEventDestination	Otorga permiso para actualizar el destino del evento de un conjunto de configuración	Write		ses:ApiVersion	
UpdateConfigurationSetReputationMetricsEnabled	Otorga permiso para habilitar o desactivar la publicación de métricas de reputación para los emails enviados mediante un conjunto de configuración específico	Write		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConfigurationSetSendingEnabled	Otorga permiso para habilitar o desactivar el envío de email para los mensajes enviados mediante un conjunto de configuración específico	Write		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	Otorga permiso para modificar una asociación entre un conjunto de configuración y un dominio personalizado para el seguimiento de eventos abiertos y de clic	Write		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	Concede permiso para actualizar una plantilla de email de verificación personalizada existente	Write		ses:ApiVersion	
UpdateReceiptRule	Otorga permiso para actualizar una regla de recepción	Write		ses:ApiVersion	
UpdateTemplate	Otorga permiso para actualizar una plantilla de email	Write		ses:ApiVersion	
VerifyDomainDkim	Otorga permiso para devolver un conjunto de tokens DKIM para un dominio	Escritura		ses:ApiVersion	
VerifyDomainIdentity	Otorga permiso para verificar un dominio	Escritura		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
VerifyEmailAddress	Otorga permiso para comprobar una dirección de email de un usuario	Escritura		ses:ApiVersion	
VerifyEmailIdentity	Otorga permiso para verificar una identidad de email	Escritura		ses:ApiVersion	

Tipos de recursos definidos por Amazon SES

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
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}`	

Tipos de recurso	ARN	Claves de condición
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Claves de condición de Amazon SES

Amazon SES define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
ses:ApiVersion	Filtra acciones basadas en la versión de la API de SES	Cadena
ses:FeedbackAddress	Filtra acciones en función de la dirección "Return-Path" (Ruta de devolución), que especifica dónde se envían los mensajes rebotados y las reclamaciones mediante el reenvío de retroalimentación por correo electrónico	Cadena
ses:FromAddress	Filtra acciones en función de la dirección "From" (Origen) de un mensaje	Cadena
ses:FromDisplayName	Filtra acciones en función de la dirección "From" (Origen) que se utiliza como nombre de visualización de un mensaje	Cadena
ses:Recipients	Filtra acciones en función de las direcciones de los destinatarios de un mensaje, que incluyen las direcciones "To" (Destino), "CC" (Copia) y "BCC" (Copia oculta).	ArrayOfString

Acciones, recursos y claves de condición para AWS Shield

AWS Shield (prefijo de servicio:`shield`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Shield
- Tipos de recursos definidos por AWS Shield
- Claves de condición para AWS Shield

Acciones definidas por AWS Shield

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*).

Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateDRTLogBucket	Otorga permiso para autorizar al equipo de DDo S Response a acceder al bucket de Amazon S3 especificado que contiene sus registros de flujo	Escritura			s3:GetBucketPolicy s3:PutBucketPolicy
AssociateDRTRole	Otorga permiso para autorizar al equipo de DDo S Response, que desempeña el rol especificado, a acceder Cuenta de AWS a usted para	Escritura			iam:GetRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	ayudarlo a mitigar los ataques de DDo S durante posibles ataques				iam:ListAttachedRolePolicies iam:PassRole
AssociateHealthCheck	Otorga permiso para agregar detección basada en el estado a la protección de Shield Advanced de un recurso.	Escritura	protection*		route53:GetHealthCheck
				aws:ResourceTag/${TagKey}	
AssociateProactiveEngagementDetails	Otorga permiso para iniciar la participación proactiva y establecer la lista de contactos para que la utilice el equipo de respuesta DDo S (DRT)	Escritura			
CreateProtection	Otorga permiso para activar el servicio de protección DDo S para un ARN de recurso determinado	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectionGroup	Otorga permiso para crear una agrupación de recursos protegidos para que puedan manejarse como un colectivo	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSubscription	Otorga permiso para activar la suscripción	Write			
DeleteProtection	Otorga permiso para eliminar una protección existente	Write	protection*		
				aws:ResourceTag/${TagKey}	
DeleteProtectionGroup	Otorga permiso para quitar el grupo de protección especificado	Write	protection-group*		
				aws:ResourceTag/${TagKey}	
DeleteSubscription	Otorga permiso para desactivar la suscripción	Write			
DescribeAttack	Otorga permiso para obtener detalles de ataque	Lectura	attack*		
DescribeAttackContributors [solo permiso]	Otorga permiso para obtener información detallada sobre las personas que contribuyen a un ataque DDoS específico	Lectura	attack*		
			protection-group		
DescribeAttackStatistics	Otorga permiso para describir información sobre el número y el tipo de ataques que AWS Shield ha detectado en el último año	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDRTAccess	Otorga permiso para describir la función actual y la lista de depósitos de registro de Amazon S3 que utiliza el equipo de DDo S Response para acceder a usted y, al Cuenta de AWS mismo tiempo, ayuda a mitigar los ataques	Lectura			
DescribeEmergencyContactSettings	Otorga permiso para mostrar las direcciones de email que el DRT puede usar a fin de contactarlo durante un presunto ataque	Read			
DescribeProtection	Otorga permiso para obtener detalles de protección	Read	protection*		
				aws:ResourceTag/${TagKey}	
DescribeProtectionGroup	Otorga permiso para describir la especificación del grupo de protección especificado	Read	protection-group*		
				aws:ResourceTag/${TagKey}	
DescribeSubscription	Otorga permiso para obtener detalles de la suscripción, como la hora de inicio	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisableApplicationLayerAutomaticResponse	Otorga permiso para desactivar la respuesta automática de capa de aplicación para la protección de Shield Advanced de un recurso	Escritura			
DisableProactiveEngagement	Otorga permiso para retirar la autorización del equipo de respuesta de DDo S (DRT) para notificar a los contactos sobre las escalaciones	Escritura			
DisassociateDRTLogBucket	Otorga permiso para eliminar el acceso del equipo de DDo S Response al bucket de Amazon S3 especificado que contiene sus registros de flujo	Escritura			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	Otorga permiso para eliminar el acceso del equipo de DDo S Response a su Cuenta de AWS	Escritura			
DisassociateHealthCheck	Otorga permiso para quitar la detección basada en el estado de la protección de Shield Advanced de un recurso	Escritura	protection*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableApplicationLayerAutomaticResponse	Otorga permiso para habilitar la respuesta automática de capa de aplicación para la protección de Shield Advanced de un recurso	Escritura			apprunner:DescribeWebAclForService cloudfront:GetDistribution cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl iam:CreateServiceLinkedRole iam:GetRole wafv2:GetWebACL wafv2:GetWebACLForResource

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
EnableProactiveEngagement	Otorga permiso para autorizar al equipo de respuesta de DDo S (DRT) a utilizar el correo electrónico y el teléfono para notificar a los contactos sobre las escaladas	Escritura			
GetGlobalThreatData [solo permiso]	Otorga permiso para recuperar datos y tendencias de inteligencia sobre amenazas globales de los sistemas de monitoreo de amenazas de AWS Shield	Lectura			
GetSubscriptionState	Otorga permiso para obtener el estado de suscripción	Read			
ListAttacks	Otorga permiso para mostrar todos los ataques existentes	Enumeración			
ListMitigations [solo permiso]	Otorga permiso para recuperar una lista de las acciones de mitigación que se han aplicado durante los ataques DDo S	Enumeración	attack*		
ListProtectionGroups	Otorga permiso para recuperar los grupos de protección de la cuenta	List			
ListProtections	Otorga permiso para mostrar todas las protecciones existentes	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourcesInProtectionGroup	Otorga permiso para recuperar los recursos incluidos en el grupo de protección	Enumeración	protection-group*		
ListTagsForResource	Otorga permiso para obtener información sobre las AWS etiquetas de un nombre de recurso de Amazon (ARN) específico en Shield AWS	Lectura	protection		
			protection-group		
TagResource	Otorga permiso para añadir o actualizar etiquetas para un recurso en AWS Shield	Etiquetado	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de un recurso en AWS Shield	Etiquetado	protection		
			protection-group		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateApplicationLayerAutomaticResponse	Otorga permiso para actualizar la respuesta automática de capa de aplicación para la protección de Shield Advanced de un recurso	Escritura			apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL wafv2:GetWebACLForResource
UpdateEmergencyContactSettings	Otorga permiso para actualizar los detalles de la lista de direcciones de email que el DRT puede utilizar a fin de contactarlo durante un presunto ataque	Write			
UpdateProtectionGroup	Otorga permiso para actualizar un grupo de protección existente	Write	protection-group*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateSubscription	Otorga permiso para actualizar los detalles de una suscripción existente	Write			

Tipos de recursos definidos por AWS Shield

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
attack	`arn:${Partition}:shield::${Account}:attack/${Id}`	
protection	`arn:${Partition}:shield::${Account}:protection/${Id}`	aws:ResourceTag/${TagKey}
protection-group	`arn:${Partition}:shield::${Account}:protection-group/${Id}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Shield

AWS Shield define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS Signer

AWS Signer (prefijo de servicio:`signer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Signer

- Tipos de recursos definidos por AWS Signer
- Claves de condición para AWS Signer

Acciones definidas por AWS Signer

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddProfilePermission	Otorga permiso para agregar permisos entre cuentas a un perfil de firma.	Permissions management	signing-profile*		
CancelSigningProfile	Otorga permiso para cambiar el estado de un perfil de firma a “CANCELED” (cancelado).	Write	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	Concede el permiso para devolver información acerca de un trabajo de firma específico.	Lectura	signing-job*		
GetRevocationStatus	Concede permiso para consultar la información de revocación de los recursos de firma	Lectura	signing-job*		
			signing-profile*		
GetSigningPlatform	Otorga permiso para devolver información acerca de una plataforma de firma específica.	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSigningProfile	Otorga permiso para devolver información acerca de un perfil de firma específico.	Read	signing-profile*		
				signer:ProfileVersion	
ListProfilePermissions	Otorga permiso para mostrar una lista de los permisos entre cuentas que estén asociados a un perfil de firma.	Read	signing-profile*		
ListSigningJobs	Otorga permiso para mostrar una lista de todos los trabajos de firma en su cuenta.	List			
ListSigningPlatforms	Otorga permiso para mostrar una lista de todas las plataformas de firma disponibles.	List			
ListSigningProfiles	Otorga permiso para mostrar una lista de todos los perfiles de firma en su cuenta.	List			
ListTagsForResource	Otorga permiso para mostrar una lista de las etiquetas asociadas a un perfil de firma.	Read	signing-profile*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutSigningProfile	Otorga permiso para crear un nuevo perfil de firma.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveProfilePermission	Otorga permiso para eliminar permisos entre cuentas de un perfil de firma.	Permissions management	signing-profile*		
RevokeSignature	Otorga permiso para cambiar el estado de un trabajo de firma a “REVOKED” (revocado).	Write	signing-job*		
				signer:ProfileVersion	
RevokeSigningProfile	Otorga permiso para cambiar el estado de un perfil de firma a “REVOKED” (revocado).	Escritura	signing-profile*		
				signer:ProfileVersion	
SignPayload	Concede permiso para iniciar un trabajo de firma en la carga proporcionada	Escritura	signing-profile*		
				signer:ProfileVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartSigningJob	Otorga permiso para iniciar un trabajo de firma en el código proporcionado.	Write	signing-profile*		
				signer:ProfileVersion	
TagResource	Otorga permiso para agregar una o varias etiquetas a un perfil de firma.	Etiquetado	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una o varias etiquetas de un perfil de firma.	Etiquetado	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Tipos de recursos definidos por AWS Signer

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
signing-profile	`arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}`	aws:ResourceTag/${TagKey}
signing-job	`arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}`	

Claves de condición para AWS Signer

AWS El firmante define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
signer:ProfileVersion	Filtra el acceso por la versión del Perfil de firma	Cadena

Acciones, recursos y claves de condición para AWS Signin

AWS El inicio de sesión (prefijo de servicio:`signin`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Signin
- Tipos de recursos definidos por AWS Signin
- Claves de condición para AWS Signin

Acciones definidas por AWS Signin

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTrustedIdentityPropagationApplicationForConsole	Otorga permiso para crear una aplicación de Identity Center que represente la instancia AWS Management Console de una organización de Identity Center	Escritura			sso:CreateApplication sso:GetSharedSsoConfiguration

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					sso:ListApplications sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
ListTrustedIdentityPropagationApplicationsForConsole	Otorga permiso para enumerar todas las aplicaciones de Identity Center que representan AWS Management Console	Enumeración			sso:GetSharedSsoConfiguration sso:ListApplications

Tipos de recursos definidos por AWS Signin

AWS El inicio de sesión no permite especificar un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso a AWS Signin, especifique `"Resource": "*"` en la política.

Claves de condición para AWS Signin

Signin no tiene claves de contexto específicas del servicio que se puedan usar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Simple Email Service - Administrador de correo electrónico

Amazon Simple Email Service - Administrador de correo electrónico (prefijo del servicio: `ses`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Simple Email Service - Administrador de correo electrónico
- Tipos de recursos definidos por Amazon Simple Email Service - Administrador de correo electrónico
- Claves de condición para Amazon Simple Email Service - Administrador de correo electrónico

Acciones definidas por Amazon Simple Email Service - Administrador de correo electrónico

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Otorga permiso para configurar la entrega de registros vendida para los recursos de Mail Manager	Administración de permisos	mailmanager-ingress-point		
			mailmanager-rule-set		
CreateAddonInstance	Concede permiso para crear una instancia de complemento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys ses:AddonSubscriptionArn	
CreateAddonSubscription	Concede permiso para crear una suscripción de complemento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAddressList	Otorga permiso para crear una lista de direcciones	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAddressListImportJob	Otorga permiso para crear un trabajo de importación en una lista de direcciones	Escritura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
CreateArchive	Concede permiso para crear un archivo	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngressPoint	Concede permiso para crear un punto de entrada	Escritura		aws:RequestTag/${TagKey} aws:TagKeys ses:MailManagerRuleSetArn ses:MailManagerTrafficPolicyArn	ec2:DescribeVpcEndpoints iam:CreateServiceLinkedRole
CreateRelay	Concede permiso para crear una retransmisión SMTP	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRuleSet	Concede permiso para crear un conjunto de reglas	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrafficPolicy	Concede permiso para crear una política de tráfico	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddonInstance	Concede permiso para eliminar una instancia de complemento	Escritura	addon-instance*		
				aws:RequestTag/${TagKey}	
DeleteAddonSubscription	Concede permiso para eliminar una suscripción de complemento	Escritura	addon-subscription*		
				aws:RequestTag/${TagKey}	
DeleteAddressList	Otorga permiso para eliminar una lista de direcciones	Escritura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteArchive	Concede permiso para eliminar un archivo	Escritura	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
DeleteIngressPoint	Concede permiso para eliminar un punto de entrada	Escritura	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
DeleteRelay	Concede permiso para eliminar una retransmisión SMTP	Escritura	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
DeleteRuleSet	Concede permiso para eliminar un conjunto de reglas	Escritura	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTrafficPolicy	Concede permiso para eliminar un punto de tráfico	Escritura	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	
DeregisterMemberFromAddressList	Otorga permiso para eliminar a un miembro de una lista de direcciones	Escritura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddonInstance	Concede permiso para obtener información sobre una instancia de complemento	Lectura	addon-instance*		
				aws:RequestTag/${TagKey}	
GetAddonSubscription	Concede permiso para obtener información sobre una suscripción de complemento	Lectura	addon-subscription*		
				aws:RequestTag/${TagKey}	
GetAddressList	Otorga permiso para obtener información sobre una lista de direcciones	Lectura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAddressListImportJob	Otorga permiso para obtener información sobre un trabajo de importación en una lista de direcciones	Lectura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetArchive	Concede permiso para obtener información sobre un archivo	Lectura	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
GetArchiveExport	Concede permiso para obtener información sobre una exportación de archivo	Lectura	mailmanager-archive*		
GetArchiveMessage	Concede permiso para recuperar un mensaje archivado	Lectura	mailmanager-archive*		
GetArchiveMessageContent	Concede permiso para recuperar el contenido de un mensaje archivado	Lectura	mailmanager-archive*		
GetArchiveSearch	Concede permiso para obtener información sobre una búsqueda	Lectura	mailmanager-archive*		
GetArchiveSearchResults	Concede permiso para obtener información sobre los resultados de la búsqueda	Lectura	mailmanager-archive*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIngressPoint	Concede permiso para obtener información sobre un punto de entrada	Lectura	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
GetMemberOfAddressList	Otorga permiso para obtener información sobre un miembro de una lista de direcciones	Lectura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetRelay	Concede permiso para obtener información sobre una retransmisión SMTP	Lectura	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
GetRuleSet	Concede permiso para obtener información sobre un conjunto de reglas	Lectura	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
GetTrafficPolicy	Concede permiso para obtener información sobre una política de tráfico	Lectura	mailmanager-traffic-policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	
ListAddonInstances	Concede permiso para enumerar todas las instancias de complemento asociadas a la cuenta	Enumeración			
ListAddonSubscriptions	Concede permiso para enumerar todas las suscripciones de complemento asociadas a la cuenta	Enumeración			
ListAddressListImportJobs	Otorga permiso para enumerar todos los trabajos de importación asociados a una lista de direcciones	Enumeración	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListAddressLists	Otorga permiso para incluir todas las listas de direcciones asociadas a su cuenta	Enumeración			
ListArchiveExports	Concede permiso para enumerar todas las exportaciones de archivos asociadas a la cuenta	Enumeración			
ListArchiveSearches	Concede permiso para enumerar todas las búsquedas de archivos asociadas a la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListArchives	Concede permiso para enumerar todos los archivos asociados a la cuenta	Enumeración			
ListIngressPoints	Concede permiso para enumerar todos los puntos de entrada asociados a la cuenta	Enumeración			
ListMembersOfAddressList	Otorga permiso para incluir todos los miembros asociados a una lista de direcciones	Enumeración	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListRelays	Concede permiso para enumerar todas las retransmisiones SMTP asociadas a la cuenta	Enumeración			
ListRuleSets	Concede permiso para enumerar todos los conjuntos de reglas asociados a la cuenta	Enumeración			
ListTagsForResource	Concede permiso para enumerar todas las etiquetas asociadas al recurso	Lectura	addon-instance		
			addon-subscription		
			mailmanager-archive		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
ListTrafficPolicies	Concede permiso para enumerar todas las políticas de tráfico asociadas a la cuenta	Enumeración			
RegisterMemberToAddressList	Otorga permiso para añadir un miembro a una lista de direcciones	Escritura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartAddressListImportJob	Otorga permiso para iniciar un trabajo de importación en una lista de direcciones	Escritura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartArchiveExport	Concede permiso para iniciar una exportación de archivo	Escritura	mailmanager-archive*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartArchiveSearch	Concede permiso para iniciar una búsqueda de archivo	Escritura	mailmanager-archive*		
StopAddressListImportJob	Otorga permiso para detener un trabajo de importación en curso en una lista de direcciones	Escritura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StopArchiveExport	Concede permiso para detener la exportación de archivo	Escritura	mailmanager-archive*		
StopArchiveSearch	Concede permiso para detener la búsqueda de archivo	Escritura	mailmanager-archive*		
TagResource	Concede permiso para agregar una o varias etiquetas (claves y valores) a un recurso especificado	Etiquetado	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permiso para eliminar una o más etiquetas (claves y valores) de un recurso especificado	Etiquetado	addon-instance		
			addon-subscription		
			mailmanager-address-list		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys	
UpdateArchive	Concede permiso para actualizar un archivo	Escritura	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
UpdateIngressPoint	Concede permiso para actualizar un punto de entrada	Escritura	mailmanager-ingress-point*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} ses:MailManagerTrafficPolicyArn ses:MailManagerRuleSetArn	
UpdateRelay	Concede permiso para actualizar una retransmisión SMTP	Escritura	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
UpdateRuleSet	Concede permiso para actualizar un conjunto de reglas	Escritura	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
UpdateTrafficPolicy	Concede permiso para actualizar una política de tráfico	Escritura	mailmanager-traffic-policy*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	

Tipos de recursos definidos por Amazon Simple Email Service - Administrador de correo electrónico

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
addon-instance	`arn:${Partition}:ses:${Region}:${Account}:addon-instance/${AddonInstanceId}`	aws:ResourceTag/${TagKey}
addon-subscription	`arn:${Partition}:ses:${Region}:${Account}:addon-subscription/${AddonSubscriptionId}`	aws:ResourceTag/${TagKey}
mailmanager-archive	`arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}`	aws:ResourceTag/${TagKey}
mailmanager-ingress-point	`arn:${Partition}:ses:${Region}:${Account}:mailmanager-ingress-point/${IngressPointId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
		ses:MailManagerIngressPointType
mailmanager-smtp-relay	arn:${Partition}:ses:${Region}:${Account}:mailmanager-smtp-relay/${RelayId}	aws:ResourceTag/${TagKey}
mailmanager-rule-set	arn:${Partition}:ses:${Region}:${Account}:mailmanager-rule-set/${RuleSetId}	aws:ResourceTag/${TagKey}
mailmanager-traffic-policy	arn:${Partition}:ses:${Region}:${Account}:mailmanager-traffic-policy/${TrafficPolicyId}	aws:ResourceTag/${TagKey}
mailmanager-address-list	arn:${Partition}:ses:${Region}:${Account}:mailmanager-address-list/${AddressListId}	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Simple Email Service - Administrador de correo electrónico

Amazon Simple Email Service - Administrador de correo electrónico define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
ses:AddonSubscriptionArn	Filtra el acceso por el ARN de suscripción de complemento de SES	ARN
ses:MailManagerIngressPointType	Filtra el acceso por tipo de punto de ingreso del Administrador de correo electrónico de SES, por ejemplo, OPEN o AUTH	Cadena
ses:MailManagerRuleSetArn	Filtra el acceso por el ARN del conjunto de reglas del Administrador de correo electrónico de SES	ARN
ses:MailManagerTrafficPolicyArn	Filtra el acceso por el ARN de la política de tráfico del Administrador de correo electrónico de SES	ARN

Acciones, recursos y claves de condición para Amazon Simple Email Service v2

Amazon Simple Email Service v2 (prefijo de servicio: `ses`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para usarse en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.

- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Simple Email Service v2
- Tipos de recursos definidos por Amazon Simple Email Service v2
- Claves de condición para Amazon Simple Email Service v2

Acciones definidas por Amazon Simple Email Service v2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las

claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetMetricData	Concede permiso para obtener datos métricos sobre su actividad	Lectura	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	Concede permiso para cancelar un trabajo de exportación	Escritura	export-job*		
				ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ExportSourceType	
CreateConfigurationSet	Otorga permiso para crear un nuevo conjunto de configuración	Write	configuration-set*		
			dedicated-ip-pool		
			mailmanager-archive		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Concede permiso para crear un destino para eventos de conjunto de configuración	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateContact	Concede permiso para crear un contacto	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContactList	Concede permiso para crear una lista de contactos	Write	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomVerificationEmailTemplate	Concede permiso para crear una nueva plantilla de email de verificación personalizada	Write	custom-verification-email-template*		
				ses:ApiVersion	
CreateDedicatedIpPool	Concede permiso para crear un grupo de direcciones IP dedicadas nuevo	Write	dedicated-ip-pool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Concede permiso para crear una prueba de colocación predictiva en la bandeja de entrada nueva	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Concede permiso para iniciar el proceso de verificación de una identidad de correo electrónico	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEmailIdentityPolicy	Concede permiso para crear la política de autorización de envío especificada para la identidad dada	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Concede permiso para crear una plantilla de email	Escritura	template*		
				ses:ApiVersion	
CreateExportJob	Concede permiso para crear un trabajo de exportación	Escritura		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	Concede permiso para crear un trabajo de importación para un destino de datos	Escritura		ses:ApiVersion	
CreateMultiRegionEndpoint	Otorga permiso para crear un nuevo punto final multirregional	Escritura		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteConfigurationSet	Concede permiso para eliminar un conjunto de configuración existente	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Concede permiso para eliminar un destino de evento	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContact	Concede permiso para eliminar un contacto de una lista de contactos	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	Concede permiso para eliminar una lista de contactos con todos sus contactos	Write	contact-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	Concede permiso para eliminar una plantilla de email de verificación personalizada existente	Write	custom-verification-email-template*		
				ses:ApiVersion	
DeleteDedicatedIpPool	Concede permiso para eliminar un grupo de IP dedicadas	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Concede permiso para eliminar una identidad de email	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteEmailIdentityPolicy	Concede permiso para eliminar la política de autorización de envío especificada para la identidad dada (una dirección de email o un dominio)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	Concede permiso para eliminar una plantilla de email	Escritura	template*		
				ses:ApiVersion	
DeleteMultiRegionEndpoint	Otorga permiso para eliminar un punto final multirregional	Escritura	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteSuppressedDestination	Concede permiso para eliminar una dirección de email de la lista de supresión de su cuenta	Write		ses:ApiVersion	
GetAccount	Concede permiso para obtener información sobre el estado del envío de un email y las capacidades de su cuenta	Read		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetBlacklistReports	Concede permiso para recuperar una lista de las listas de denegación en las que aparecen sus direcciones IP dedicadas o dominios de seguimiento	Read		ses:ApiVersion	
GetConfigurationSet	Concede permiso para obtener información sobre un conjunto de configuración existente	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Concede permiso para recuperar una lista de destinos de eventos que están asociados con un conjunto de configuración	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContact	Concede permiso para devolver un contacto de una lista de contactos	Read	contact-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	Concede permiso para devolver metadatos de una lista de contactos	Read	contact-list*		
				ses:ApiVersion	
GetCustomVerificationEmailTemplate	Concede permiso para devolver la plantilla personalizada de verificación de email para el nombre de plantilla especificado	Read	custom-verification-email-template*		
				ses:ApiVersion	
GetDedicatedIp	Concede permiso para obtener información sobre una dirección IP dedicada	Lectura		ses:ApiVersion	
GetDedicatedIpPool	Concede permiso para obtener información sobre un grupo de IP dedicadas	Lectura	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDedicatedIps	Concede permiso para enumerar las direcciones IP dedicadas en un grupo de IP dedicadas	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Concede permiso para obtener el estado del panel de capacidad de entrega	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Concede permiso para recuperar los resultados de una prueba de colocación predictiva en la bandeja de entrada	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Concede permiso para recuperar todos los datos de capacidad de entrega de una campaña específica	Read		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetDomainStatisticsReport	Concede permiso para recuperar la ubicación de la bandeja de entrada y las tasas de interacción de los dominios que utiliza para enviar correos electrónicos	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Concede permiso para obtener información acerca de una identidad especificada	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	Concede permiso para devolver las políticas de autorización de envío solicitadas para la identidad dada (una dirección de email o un dominio)	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailTemplate	Concede permiso para devolver el objeto de plantilla, que incluye la línea de asunto, parte en HTML y parte de texto, para la plantilla especificada	Lectura	template*		
				ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetExportJob	Concede permiso para obtener información sobre un trabajo de exportación	Lectura	export-job*		
				ses:ApiVersion ses:ExportSourceType	
GetImportJob	Concede permiso para proporcionar información sobre un trabajo de importación	Lectura	import-job*		
				ses:ApiVersion	
GetMessageInsights	Concede permiso para proporcionar información sobre un mensaje	Lectura		ses:ApiVersion	
GetMultiRegionEndpoint	Otorga permiso para obtener información sobre un punto final multirregional	Lectura	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSuppressedDestination	Concede permiso para recuperar información sobre una dirección de email específica que está en la lista de supresión de su cuenta	Read		ses:ApiVersion	
ListConfigurationSets	Concede permiso para enumerar todos los conjuntos de configuración de su cuenta	List		ses:ApiVersion	
ListContactLists	Concede permiso para enumerar todas las listas de contactos disponibles para su cuenta	List		ses:ApiVersion	
ListContacts	Concede permiso para enumerar los contactos presentes en una lista de contactos específica	List	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	Concede permiso para enumerar todas las plantillas de email de verificación personalizadas existentes para su cuenta	List		ses:ApiVersion	
ListDedicatedIpPools	Concede permiso para enumerar todos los grupos de IP dedicadas para su cuenta	List		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDeliverability TestReports	Concede permiso para recuperar la lista de las pruebas de colocación predictivas en la bandeja de entrada que haya realizado en la cuenta, independientemente de sus estados	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Concede permiso para enumerar los datos de capacidad de entrega de las campañas que utilizaron un dominio específico para enviar emails durante un periodo específico	Read		ses:ApiVersion	
ListEmailIdentities	Concede permiso para enumerar las identidades de email de su cuenta	List		ses:ApiVersion	
ListEmailTemplates	Concede permiso para enumerar todas las plantillas de email de su cuenta	Enumeración		ses:ApiVersion	
ListExportJobs	Concede permiso para enumerar todos los trabajos de exportación de su cuenta	Enumeración		ses:ApiVersion ses:ExportSourceType	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListImportJobs	Concede permiso para enumerar todos los trabajos de importación de su cuenta	Enumeración		ses:ApiVersion	
ListMultiRegionEndpoints	Otorga permiso para enumerar todos los puntos de conexión multirregionales de su cuenta	Enumeración		ses:ApiVersion	
ListRecommendations	Concede permiso para enumerar las recomendaciones de lista para su cuenta	Lectura	identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	Concede permiso para enumerar las direcciones de email que están en la lista de supresión de su cuenta	Read		ses:ApiVersion	
ListTagsForResource	Concede permiso para recuperar una lista de las etiquetas (claves y valores) asociadas a un recurso específico para su cuenta	Read	configuration-set		
			contact-list		
			dedicated-ip-pool		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			deliverability-test-report		
			identity		
				ses:ApiVersion	
PutAccountDedicatedIpWarmupAttributes	Concede permiso para habilitar o desactivar la característica de preparación automática para direcciones IP dedicadas	Write		ses:ApiVersion	
PutAccountDetails	Concede permiso para actualizar los detalles de su cuenta	Write		ses:ApiVersion	
PutAccountSendingAttributes	Concede permiso para habilitar o desactivar la capacidad de envío de emails para su cuenta	Write		ses:ApiVersion	
PutAccountSuppressionAttributes	Concede permiso para cambiar la configuración de la lista de supresión al nivel de la cuenta	Escritura		ses:ApiVersion	
PutAccountVdmAttributes	Concede permiso para cambiar la configuración de VDM de su cuenta	Escritura		ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConfigurationSetArchivingOptions	Otorga permiso para asociar un conjunto de configuraciones a un archivo de Mail Manager	Escritura	configuration-set*		
			mailmanager-archive		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetDeliveryOptions	Concede permiso para asociar un conjunto de configuración a un grupo de IP dedicadas	Write	configuration-set*		
			dedicated-ip-pool		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConfigurationSetReputationOptions	Concede permiso para habilitar o desactivar la recopilación de métricas de reputación para los correos electrónicos que envía a través de un conjunto de configuración determinado	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	Concede permiso para habilitar o desactivar el envío de correos electrónicos para mensajes que utilizan un conjunto de configuración determinado	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSuppressionOptions	Concede permiso para especificar las preferencias de la lista de supresión de cuentas para un conjunto de configuración determinado	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutConfigurationSetTrackingOptions	Concede permiso para especificar un dominio personalizado que se utilizará para los elementos de seguimiento de clic y de apertura en el email que envíe para un conjunto de configuración determinado	Escritura	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetVdmOptions	Concede permiso para anular la configuración del VDM a nivel de la cuenta para un conjunto de configuración determinado	Escritura	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Concede permiso para mover una dirección IP dedicada a un grupo de IP dedicadas existente	Escritura	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	Concede permiso para convertir un grupo de IP dedicadas de estándar a administradas	Escritura	dedicated-ip-pool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Concede permiso para poner atributos de preparación de IP dedicadas	Write		ses:ApiVersion	
PutDeliverabilityDashboardOption	Concede permiso para habilitar o desactivar el panel de capacidad de entrega	Write		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	Concede permiso para asociar un conjunto de configuración con una identidad de email	Write	identity*		
			configuration-set		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutEmailIdentityDkimAttributes	Concede permiso para habilitar o desactivar la autenticación DKIM para una identidad de correo electrónico	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimSigningAttributes	Concede permiso para configurar o cambiar la configuración de la autenticación DKIM para una identidad de dominio de email	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Concede permiso para habilitar o desactivar el reenvío de comentarios para una identidad de email	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Concede permiso para habilitar o desactivar la configuración de dominio MAIL FROM personalizada para una identidad de correo electrónico	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutSuppressedDestination	Concede permiso para agregar una dirección de email a la lista de supresión	Escritura		ses:ApiVersion	
ReplicateEmailIdentityDkimSigningKey [solo permiso]	Otorga permiso para replicar la clave de firma DKIM de identidad del correo electrónico	Administración de permisos	identity*		
				ses:ReplicaRegion	
SendBulkEmail	Concede permiso para redactar un mensaje de email para varios destinos	Write	identity*		
			template*		
			configuration-set		
				ses:ApiVersion ses:MultiRegionEndpointId	
SendCustomVerificationEmail	Concede permiso para agregar una dirección de email a la lista de identidades e intenta verificarla	Write	custom-verification-email-template*		
				ses:ApiVersion	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendEmail	Concede permiso para enviar un mensaje de correo electrónico	Write	identity*		
			configuration-set		
			template		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients ses:MultiRegionEndpointId	
TagResource	Concede permiso para agregar una o varias etiquetas (claves y valores) a un recurso especificado	Etiquetado	configuration-set		
			contact-list		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
TestRenderEmailTemplate	Concede permiso para crear una vista previa del contenido MIME de un email cuando se proporciona con una plantilla y un conjunto de datos de sustitución	Write	template*		
				ses:ApiVersion	
UntagResource	Concede permiso para eliminar una o más etiquetas (claves y valores) de un recurso especificado	Etiquetado	configuration-set		
			contact-list		
			dedicated-ip-pool		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Concede permiso para actualizar la configuración de un destino de eventos para un conjunto de configuración	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	Concede permiso para actualizar las preferencias de un contacto para una lista	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContactList	Concede permiso para actualizar los metadatos de la lista de contactos	Write	contact-list*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	Concede permiso para actualizar una plantilla de email de verificación personalizada existente	Write	custom-verification-email-template*		
				ses:ApiVersion	
UpdateEmailIdentityPolicy	Concede permiso para actualizar la política de autorización de envío especificada para la identidad dada (una dirección de email o un dominio)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	Concede permiso para actualizar una plantilla de email	Write	template*		
				ses:ApiVersion	

Tipos de recursos definidos por Amazon Simple Email Service v2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
contact-list	`arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}`	aws:ResourceTag/${TagKey}
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
export-job	`arn:${Partition}:ses:${Region}:${Account}:export-job/${ExportJobId}`	
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey}
import-job	`arn:${Partition}:ses:${Region}:${Account}:import-job/${ImportJobId}`	
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Tipos de recurso	ARN	Claves de condición
multi-region-endpoint	`arn:${Partition}:ses:${Region}:${Account}:multi-region-endpoint/${EndpointName}`	
mailmanager-archive	`arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Simple Email Service v2

Amazon Simple Email Service v2 define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
ses:ApiVersion	Filtra el acceso según la versión de la API de SES	Cadena
ses:ExportSourceType	Filtra el acceso según el tipo de fuente de exportación	Cadena

Claves de condición	Descripción	Tipo
ses:FeedbackAddress	Filtra el acceso según la dirección "Return-Path" (Ruta de devolución), que especifica dónde se envían los mensajes rebotados y las reclamaciones mediante el reenvío de retroalimentación por correo electrónico	Cadena
ses:FromAddress	Filtra el acceso según la dirección "From" (Origen) de un mensaje	Cadena
ses:FromDisplayName	Filtra el acceso según la dirección "From" (Origen) que se utiliza como nombre de visualización de un mensaje	Cadena
ses:MultiRegionEndpointId	Filtra el acceso por el identificador de punto final multirregional que se utiliza para enviar el correo electrónico	Cadena
ses:Recipients	Filtra el acceso según las direcciones de los destinatarios de un mensaje, que incluyen las direcciones "To" (Destino), "CC" (Copia) y "BCC" (Copia oculta)	ArrayOfString
ses:ReplicaRegion	Filtra el acceso por regiones de réplica para replicar la clave de firma DKIM del dominio	ArrayOfString

Acciones, recursos y claves de condición para Amazon Simple Workflow Service

Amazon Simple Workflow Service (prefijo de servicio: `swf`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos de servicios para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Simple Workflow Service
- Tipos de recursos definidos por Amazon Simple Workflow Service
- Claves de condición para Amazon Simple Workflow Service

Acciones definidas por Amazon Simple Workflow Service

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelTimer [solo permiso]	Otorga permiso para cancelar un temporizador iniciado anteriormente y registrar un TimerCanceled evento en el historial	Escritura	domain*		
CancelWorkflowExecution [solo permiso]	Otorga permiso para cerrar la ejecución del flujo de trabajo y registrar un WorkflowExecutionCanceled evento en el historial	Escritura	domain*		
CompleteWorkflowExecution [solo permiso]	Otorga permiso para cerrar la ejecución del flujo de trabajo y registrar un WorkflowExecutionCompleted evento en el historial	Escritura	domain*		
ContinueAsNewWorkflowExecut	Concede permiso para cerrar la ejecución del flujo de trabajo e iniciar una nueva	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ion [solo permiso]	ejecución de flujo de trabajo del mismo tipo utilizando el mismo ID de flujo de trabajo y un ID de ejecución exclusivo				
CountClosedWorkflowExecutions	Concede permiso para devolver el número de ejecuciones de flujo de trabajo cerradas en el dominio dado que cumplen los criterios de filtrado especificados	Lectura	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountOpenWorkflowExecutions	Concede permiso para devolver el número de ejecuciones de flujo de trabajo abiertas en el dominio dado que cumplen los criterios de filtrado especificados	Lectura	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CountPendingActivityTasks	Concede permiso para devolver el número estimado de las tareas de actividad de la lista de tareas especificada	Lectura	domain*		
				swf:taskList.name	
CountPendingDecisionTasks	Concede permiso para devolver el número estimado de las tareas de decisión de la lista de tareas especificada	Lectura	domain*		
				swf:taskList.name	
DeleteActivityType	Concede permiso para eliminar el tipo de actividad especificado	Escritura	domain*		
				swf:activityType.name swf:activityType.version	
DeleteWorkflowType	Concede permiso para eliminar el tipo de flujo de trabajo especificado	Escritura	domain*		
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	Concede permiso para dar de baja el tipo de actividad especificado	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				swf:activityType.name swf:activityType.version	
DeprecateDomain	Concede permiso para dar de baja el tipo de dominio especificado	Escritura	domain*		
DeprecateWorkflowType	Concede permiso para dar de baja el tipo de flujo de trabajo especificado	Escritura	domain*		
				swf:workflowType.name swf:workflowType.version	
DescribeActivityType	Concede permiso para devolver información acerca del tipo de actividad especificado	Lectura	domain*		
				swf:activityType.name swf:activityType.version	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDomain	Concede permiso para devolver información sobre el dominio especificado, incluidos la descripción y el estado	Lectura	domain*		
DescribeWorkflowExecution	Concede permiso para devolver información sobre la ejecución del flujo de trabajo especificado, incluidos su tipo y algunas estadísticas	Lectura	domain*		
DescribeWorkflowType	Concede permiso para devolver información sobre el tipo de flujo de trabajo especificado	Lectura	domain*		
				swf:workflowType.name swf:workflowType.version	
FailWorkflowExecution [solo permiso]	Otorga permiso para cerrar la ejecución del flujo de trabajo y registrar un WorkflowExecutionFailed evento en el historial	Escritura	domain*		
GetWorkflowExecutionHistory	Concede permiso para devolver el historial de la ejecución del flujo de trabajo especificado	Lectura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListActivityTypes	Concede permiso para devolver información sobre todas las actividades registradas en el dominio especificado que coinciden con el nombre y estado de registro especificados	Enumeración	domain*		
ListClosedWorkflowExecutions	Concede permiso para devolver una lista de las ejecuciones de flujo de trabajo cerradas en el dominio especificado que cumplen los criterios de filtrado	Enumeración	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListDomains	Concede permiso para devolver la lista de los dominios registrados en la cuenta	Enumeración			
		Enumeración	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListOpenWorkflowExecutions	Concede permiso para devolver una lista de las ejecuciones de flujo de trabajo abiertas en el dominio especificado que cumplen los criterios de filtrado			swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un AWS recurso SWF	Enumeración	domain		
ListWorkflowTypes	Concede permiso para devolver información acerca de los tipos de flujo de trabajo en el dominio especificado	Enumeración	domain*		
PollForActivityTask	Concede permiso a los trabajadores para obtener una ActivityTask TaskList de la actividad especificada	Escritura	domain*		
				swf:taskList.name	
PollForDecisionTask	Otorga permiso a los decisores para obtener una DecisionTask TaskList de la decisión especificada	Escritura	domain*		
				swf:taskList.name	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RecordActivityTaskHeartbeat	Concede permiso a los trabajadores para informar al servicio de que lo ActivityTask representado por el TaskToken especificado sigue progresando	Escritura	domain*		
RecordMarker [solo permiso]	Otorga permiso para grabar un MarkerRecorded evento en el historial	Escritura	domain*		
RegisterActivityType	Concede permiso para registrar un nuevo tipo de actividad junto con sus valores de configuración en el dominio especificado	Escritura	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	Concede permiso para registrar un nuevo dominio	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterWorkflowType	Concede permiso para registrar un nuevo tipo de flujo de trabajo y sus valores de configuración en el dominio especificado	Escritura	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [solo permiso]	Concede permiso para intentar cancelar una tarea de actividad programada anteriormente	Escritura	domain*		
RequestCancelExternalWorkflowExecution [solo permiso]	Concede permiso para solicitar que se cancele la ejecución especificada del flujo de trabajo externo	Escritura	domain*		
RequestCancelWorkflowExecution	Otorga permiso para grabar un WorkflowExecutionCancelRequested evento en la ejecución del flujo de trabajo actualmente en ejecución identificado por el dominio, WorkFlowid y RunID proporcionados	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RespondActivityTaskCanceled	Concede permiso a los trabajadores para informar al servicio de que lo ActivityTask identificado por el TaskToken se ha cancelado correctamente	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RespondActivityTaskCompleted	Otorga permiso a los trabajadores para indicar al servicio que lo ActivityTask identificado por el TaskToken se ha completado correctamente con un resultado (si se ha proporcionado)	Escritura	domain*	swf:activityType.name swf:activityType.version swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	Otorga permiso a los trabajadores para informar al servicio de que lo ActivityTask identificado por el TaskToken ha fallado por el motivo (si se especifica)	Escritura	domain*		
RespondDecisionTaskCompleted	Otorga permiso a los decisores para indicar al servicio que lo DecisionTask identificado por el TaskToken se ha completado correctamente	Escritura	domain*		
ScheduleActivityTask [solo permiso]	Concede permiso para programar una tarea de actividad	Escritura	domain*		
SignalExternalWorkflowExecution [solo permiso]	Concede permiso para solicitar que se entregue una señal a la ejecución y registros del flujo de trabajo externo especificados	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SignalWorkflowExecution	Otorga permiso para registrar un WorkflowExecutionSignaled evento en el historial de ejecución del flujo de trabajo y crear una tarea de decisión para la ejecución del flujo de trabajo identificada por el dominio dado, workflowID y runID	Escritura	domain*		
StartChildWorkflowExecution [solo permiso]	Concede permiso para solicitar que se inicie la ejecución de un flujo de trabajo secundario	Escritura	domain*		
StartTimer [solo permiso]	Concede permiso para iniciar un temporizador para la ejecución del flujo de trabajo	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartWorkflowExecution	Concede permiso para iniciar una ejecución del tipo de flujo de trabajo en el dominio especificado mediante el workflowId y los datos de entrada proporcionados	Escritura	domain*	swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name swf:workflowType.name swf:workflowType.version	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar un recurso SWF AWS	Etiquetado	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	Otorga permiso para registrar un WorkflowExecutionTerminated evento y forzar el cierre de la ejecución del flujo de trabajo identificada por el dominio, runID y WorkflowID dados	Escritura	domain*		
UndeprecateActivityType	Concede permiso para volver a utilizar un tipo de actividad previamente dado de baja	Escritura	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	Concede permiso para volver a utilizar un dominio previamente dado de baja	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UndeprecateWorkflowType	Concede permiso para volver a utilizar un tipo de flujo de trabajo previamente dado de baja	Escritura	domain*		
				swf:workflowType.name swf:workflowType.version	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso SWF AWS	Etiquetado	domain		
				aws:TagKeys	

Tipos de recursos definidos por Amazon Simple Workflow Service

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Simple Workflow Service

Amazon Simple Workflow Service define las siguientes claves de condiciones que se puede utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por la etiqueta del recurso	Cadena
aws:TagKeys	Filtra el acceso por la etiqueta de la clave	ArrayOfString
swf:activityType.name	Filtra el acceso por el nombre del tipo de actividad	Cadena
swf:activityType.version	Filtra el acceso por la versión del tipo de actividad	Cadena
swf:defaultTaskList.name	Filtra el acceso por el nombre de la lista de tareas predeterminada	Cadena
swf:name	Filtra el acceso por el nombre de las actividades o los flujos de trabajo	Cadena
swf:tagFilter.tag	Filtra el acceso por el valor de la etiqueta tagFilter	Cadena
swf:tagList.member.0	Filtra el acceso por la etiqueta especificada	Cadena

Claves de condición	Descripción	Tipo
swf:tagList.member.1	Filtra el acceso por la etiqueta especificada	Cadena
swf:tagList.member.2	Filtra el acceso por la etiqueta especificada	Cadena
swf:tagList.member.3	Filtra el acceso por la etiqueta especificada	Cadena
swf:tagList.member.4	Filtra el acceso por la etiqueta especificada	Cadena
swf:taskList.name	Filtra el acceso por el nombre de la lista de tareas	Cadena
swf:typeFilter.name	Filtra el acceso por el nombre del tipo de filtro	Cadena
swf:typeFilter.version	Filtra el acceso por la versión del tipo de filtro	Cadena
swf:version	Filtra el acceso por la versión de las actividades o los flujos de trabajo	Cadena
swf:workflowType.name	Filtra el acceso por el nombre del tipo de flujo de trabajo	Cadena
swf:workflowType.version	Filtra el acceso por la versión del tipo de flujo de trabajo	Cadena

Acciones, recursos y claves de condición de Amazon SimpleDB

Amazon SimpleDB (prefijo de servicio: `sdb`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon SimpleDB
- Tipos de recurso definidos por Amazon SimpleDB
- Claves de condición de Amazon SimpleDB

Acciones definidas por Amazon SimpleDB

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDeleteAttributes	Realiza varias DeleteAttributes operaciones en una sola llamada, lo que reduce los viajes de ida y vuelta y las latencias	Escritura	domain*		
BatchPutAttributes	Con la BatchPutAttributes operación, puede realizar múltiples PutAttribute operaciones en una sola llamada. Con la BatchPutAttributes operación, puede realizar múltiples PutAttribute operaciones en una sola llamada	Escritura	domain*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDomain	La CreateDomain operación crea un nuevo dominio	Escritura	domain*		
DeleteAttributes	Elimina uno o varios atributos asociados al elemento	Escritura	domain*		
DeleteDomain	La DeleteDomain operación elimina un dominio	Escritura	domain*		
DomainMetadata	Devuelve información sobre el dominio, incluido cuándo se creó el dominio, el número de elementos y atributos, y el tamaño de los nombres y valores de los atributos	Lectura	domain*		
GetAttributes	Devuelve todos los atributos asociados al elemento	Lectura	domain*		
ListDomains	Descripción de ListDomains	Enumeración			
PutAttributes	La PutAttributes operación crea o reemplaza los atributos de un elemento	Escritura	domain*		
Select	Descripción de selección	Read	domain*		

Tipos de recurso definidos por Amazon SimpleDB

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso

también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
domain	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	

Claves de condición de Amazon SimpleDB

SimpleDB no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Claves de condición, recursos y acciones de AWS SimSpace Weaver

AWS SimSpace Weaver (prefijo de servicio:`simspaceweaver`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Weaver AWS SimSpace
- Tipos de recursos definidos por Weaver AWS SimSpace
- Claves de condición para Weaver AWS SimSpace

Acciones definidas por Weaver AWS SimSpace

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSnapshot	Concede permiso para crear una instantánea	Escritura	Simulation*		
DeleteApp	Otorga permiso para eliminar una aplicación	Escritura	Simulation*		
DeleteSimulation	Otorga permiso para eliminar una simulación.	Escritura	Simulation*		
DescribeApp	Otorga permiso para describir una aplicación	Lectura	Simulation*		
DescribeSimulation	Otorga permiso para describir una simulación.	Lectura	Simulation*		
ListApps	Otorga permiso para enumerar aplicaciones	Lectura	Simulation*		
ListSimulations	Otorga permiso para enumerar simulaciones.	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
StartApp	Otorga permiso para iniciar una aplicación	Escritura	Simulation*		
StartClock	Otorga permiso para iniciar un reloj de simulación.	Escritura	Simulation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartSimulation	Otorga permiso para iniciar una simulación.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
StopApp	Otorga permiso para detener una aplicación	Escritura	Simulation*		
StopClock	Otorga permiso para detener un reloj de simulación.	Escritura	Simulation*		
StopSimulation	Otorga permiso para detener una simulación.	Escritura	Simulation*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	Simulation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	Simulation*		
				aws:TagKeys	

Tipos de recursos definidos por Weaver AWS SimSpace

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Simulation	`arn:${Partition}:simspaceweaver:${Region}:${Account}:simulation/${SimulationName}`	aws:ResourceTag/${TagKey}

Claves de condición para Weaver AWS SimSpace

AWS SimSpace Weaver define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Snow Device Management

AWS Snow Device Management (prefijo de servicio:`snow-device-management`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Snow Device Management
- Tipos de recursos definidos por AWS Snow Device Management
- Claves de condición para AWS Snow Device Management

Acciones definidas por AWS Snow Device Management

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelTask	Otorga permiso para cancelar tareas en dispositivos remotos	Escritura	task*		
CreateTask	Otorga permiso para crear tareas en dispositivos remotos	Escritura		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeDevice	Otorga permiso para describir un dispositivo administrado de forma remota	Lectura	managed-device*		
DescribeDeviceEc2Instances	Otorga permiso para describir las instancias de un dispositivo gestionado de forma remota EC2	Lectura	managed-device*		
DescribeExecution	Otorga permiso para describir las ejecuciones de las tareas	Lectura			
DescribeTask	Otorga permiso para describir una tarea	Lectura	task*		
ListDeviceResources	Otorga permiso para enumerar los recursos de un dispositivo administrado de forma remota	Enumeración	managed-device*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDevices	Otorga permiso para enumerar dispositivos administrados de forma remota	Enumeración			
ListExecutions	Otorga permiso para enumerar las ejecuciones de las tareas	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso (dispositivo o tarea)	Lectura		aws:RequestTag/${TagKey} aws:TagKeys	
ListTasks	Otorga permiso para enumerar las tareas	Enumeración			
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	managed-device		
			task		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar etiquetas en un recurso	Etiquetado	managed-device		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			task		
				aws:TagKeys	

Tipos de recursos definidos por AWS Snow Device Management

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
managed-device	`arn:${Partition}:snow-device-management:${Region}:${Account}:managed-device/${ResourceId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:snow-device-management:${Region}:${Account}:task/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Snow Device Management

AWS Snow Device Management define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la presencia de los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Snowball

AWS Snowball (prefijo de servicio:`snowball`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Snowball
- Tipos de recursos definidos por AWS Snowball
- Claves de condición para AWS Snowball

Acciones definidas por AWS Snowball

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelCluster	Concede permiso para cancelar un trabajo de clúster	Escritura			
CancelJob	Concede permiso para cancelar el trabajo especificado	Escritura			
CreateAddress	Concede permiso para crear una dirección para un Snowball al que enviar	Escritura			
CreateCluster	Concede permiso para crear un clúster vacío	Escritura			
CreateJob	Concede permiso para crear una tarea para importar o exportar datos entre Amazon S3 y su centro de datos local	Escritura			
CreateLongTermPricing	Otorga permiso LongTermPricingListEntry para crear una que permita a los clientes añadir un contrato de facturación por adelantado para un trabajo	Escritura			
CreateReturnShippingLabel	Otorga permiso para crear una etiqueta de envío que se utilizará para devolver el dispositivo Snow a AWS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAddress	Concede permiso para obtener detalles específicos sobre esa dirección en forma de objeto Address	Lectura			
DescribeAddresses	Concede permiso para describir un número especificado de objetos ADDRESS	Enumeración			
DescribeCluster	Concede permiso para describir información sobre un clúster específico que incluye información de envío, estado del clúster y otros metadatos importantes	Lectura			
DescribeJob	Concede permiso para describir información sobre un trabajo específico que incluye información de envío, estado del trabajo y otros metadatos importantes	Lectura			
DescribeReturnShippingLabel	Otorga permiso para describir la información que figura en la etiqueta de envío de un dispositivo Snow que se devuelva a AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetJobManifest	Otorga permiso para obtener un enlace a una URL prefirmada de Amazon S3 para el archivo de manifiesto asociado al valor especificado JobId	Lectura			
GetJobUnlockCode	Otorga permiso para obtener el valor de UnlockCode código del trabajo especificado	Lectura			
GetSnowballUsage	Concede permiso para obtener información sobre el límite del servicio Snowball para la cuenta, así como el número de instancias de Snowball que está utilizando la cuenta	Lectura			
GetSoftwareUpdates	Otorga permiso para devolver una URL prefirmada de Amazon S3 para un archivo de actualización asociado a un archivo especificado JobId	Lectura			
ListClusterJobs	Otorga permiso para enumerar JobListEntry objetos de la longitud especificada	Enumeración			
ListClusters	Otorga permiso para enumerar ClusterListEntry objetos de la longitud especificada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListCompatibleImages	Concede permiso para devolver una lista de las diferentes EC2 Amazon Amazon Machine Images (AMIs) de su propiedad y Cuenta de AWS que podrían utilizarse en un dispositivo Snow	Enumeración			
ListJobs	Otorga permiso para enumerar JobListEntry objetos de la longitud especificada	Enumeración			
ListLongTermPricing	Otorga permiso para enumerar LongTermPricingListEntry objetos a la cuenta que realiza la solicitud	Lectura			
ListPickupLocations	Otorga permiso para enumerar los objetos de dirección en los que se encuentra disponible la recolección, de la longitud especificada	Enumeración			
ListServiceVersions	Concede permiso para enumerar todas las versiones compatibles con servicios en dispositivo de Snow	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCluster	Otorga permiso para actualizar mientras el ClusterState valor de un clúster esté en ese AwaitingQuorum estado, puede actualizar parte de la información asociada a un clúster	Escritura			
UpdateJob	Otorga permiso para actualizar. Si el JobState valor de un trabajo es Nuevo, puede actualizar parte de la información asociada a un trabajo	Escritura			
UpdateJobShipmentState	Concede permiso para actualizar el estado cuando el estado de un envío cambia a otro estado	Escritura			
UpdateLongTermPricing	Otorga permiso para actualizar un contrato de facturación inicial específico para un trabajo	Escritura			

Tipos de recursos definidos por AWS Snowball

AWS Snowball no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Snowball, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Snowball

Snowball no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condiciones AWS globales.

Acciones, recursos y claves de condición para Amazon SNS

Amazon SNS (prefijo de servicio: `sns`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicas del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon SNS
- Tipos de recurso definidos por Amazon SNS
- Claves de condición de Amazon SNS

Acciones definidas por Amazon SNS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddPermission	Otorga permiso para añadir una declaración a la política de control de acceso de un tema, lo que permite el acceso de las AWS cuentas especific	Administración de permisos	topic*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	adas a las acciones especificadas				
CheckIfPhoneNumberIsOptedOut	Otorga permiso para aceptar un número de teléfono e indicar si el titular del teléfono ha cancelado la suscripción de recibir mensajes SMS desde su cuenta	Read			
ConfirmSubscription	Otorga permiso para verificar la intención del propietario de un punto de enlace de recibir mensajes al validar el token enviado al punto de enlace por una acción de suscripción anterior	Write	topic*		
CreatePlatformApplication	Otorga permiso para crear un objeto de aplicación de plataforma para uno de los servicios de notificación de inserción admitidos, como APNS o GCM, en el que se pueden registrar dispositivos y aplicaciones móviles	Write			iam:PassRole
CreatePlatformEndpoint	Otorga permiso para crear un punto de enlace para un dispositivo y una aplicación móvil en uno de los servicios de notificación de inserción admitidos, como GCM y APNS	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSMSSandboxPhoneNumber	Otorga permiso para añadir un número de teléfono de destino y enviar una contraseña de un solo uso (OTP) a ese número de teléfono para un Cuenta de AWS	Escritura			
CreateTopic	Otorga permiso para crear un tema en el que se pueden publicar notificaciones	Write	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEndpoint	Otorga permiso para eliminar el punto de enlace de un dispositivo y de una aplicación móvil de Amazon SNS	Write			
DeletePlatformApplication	Otorga permiso para eliminar un objeto de aplicación de plataforma para uno de los servicios de notificación de inserción admitidos, como APNS y GCM	Escritura			
DeleteSMSSandboxPhoneNumber	Otorga permiso para eliminar un número Cuenta de AWS de teléfono verificado o pendiente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTopic	Otorga permiso para eliminar un tema y todas sus suscripciones	Escritura	topic*		
GetDataProtectionPolicy	Otorga permiso para devolver la política de protección de datos del tema	Lectura	topic*		
GetEndpointAttributes	Otorga permiso para recuperar los atributos de punto de enlace para un dispositivo en uno de los servicios de notificación de inserción admitidos, como GCM y APNS	Read			
GetPlatformApplicationAttributes	Otorga permiso para recuperar los atributos del objeto de aplicación de plataforma para los servicios de notificación de inserción admitidos, como APNS y GCM	Read			
GetSMSAttributes	Otorga permiso para devolver la configuración para enviar mensajes SMS desde su cuenta	Read			
GetSMSSandboxAccountStatus	Otorga permiso para recuperar el estado del entorno limitado de la cuenta de llamada en la región de destino	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSubscriptionAttributes	Otorga permiso para devolver todas las propiedades de una suscripción	Read			
GetTopicAttributes	Otorga permiso para devolver todas las propiedades de un tema	Read	topic*		
ListEndpointsByPlatformApplication	Otorga permiso para enumerar los puntos de enlace y los atributos de los puntos de enlace de los dispositivos de un servicio de notificaciones de inserción compatible, como GCM y APNS	List			
ListOriginationNumbers	Otorga permiso para enumerar todos los números de origen y sus metadatos	List			
ListPhoneNumbersOptedOut	Otorga permiso para devolver una lista de números de teléfono cuya suscripción se ha cancelado, lo que significa que no les puede enviar mensajes SMS	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPlatformApplications	Otorga permiso para enumerar los objetos de aplicación de plataforma para los servicios de notificación de inserción admitidos, como APNS y GCM	List			
ListSMSSandboxPhoneNumbers	Otorga permiso para enumerar los números de teléfono de destino actuales pendientes y verificados de la cuenta de llamada	List			
ListSubscriptions	Otorga permiso para devolver una lista de las suscripciones del solicitante	List			
ListSubscriptionsByTopic	Otorga permiso para devolver una lista de las suscripciones a un tema específico	List	topic*		
ListTagsForResource	Otorga permiso para enumerar todas las etiquetas agregadas al tema de Amazon SNS especificado	Read	topic		
ListTopics	Otorga permiso para devolver una lista de los temas del solicitante	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
OptInPhoneNumber	Otorga permiso para dar de alta un número de teléfono que actualmente está desactivado, lo que le permitirá volver a enviar mensajes SMS al número	Write			
Publish	Otorga permiso para enviar un mensaje a todos los puntos de enlace suscritos de un tema	Escritura	topic*		
PutDataProtectionPolicy	Otorga permiso para permitir que un propietario de tema establezca la política de protección de datos	Escritura	topic*		
RemovePermission	Otorga permiso para eliminar una instrucción de la política de control de acceso de un tema	Permissions management	topic*		
SetEndpointAttributes	Otorga permiso para establecer los atributos para un punto de enlace para un dispositivo en uno de los servicios de notificación de inserción admitidos, como GCM y APNS	Write			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SetPlatformApplicationAttributes	Otorga permiso para establecer los atributos del objeto de aplicación de plataforma para los servicios de notificación de inserción admitidos, como APNS y GCM	Write			iam:PassRole
SetSMSAttributes	Otorga permiso para establecer la configuración predeterminada para enviar mensajes SMS y recibir informes diarios de uso de SMS	Write			
SetSubscriptionAttributes	Otorga permiso para permitir que el propietario de una suscripción establezca un atributo del tema en un nuevo valor	Write			
SetTopicAttributes	Otorga permiso para permitir que un propietario de tema establezca un atributo del tema en un nuevo valor	Administración de permisos	topic*		iam:PassRole
Subscribe	Otorga permiso para prepararse para suscribir un punto de enlace al enviarle a este un mensaje de confirmación	Write	topic*		
				sns:Endpoint sns:Protocol	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para agregar etiquetas al tema de Amazon SNS especificado	Etiquetado	topic		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	Otorga permiso para eliminar una suscripción	Write			
UntagResource	Otorga permiso para eliminar etiquetas del tema de Amazon SNS especificado	Etiquetado	topic		
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	Otorga permiso para verificar un número de teléfono de destino con una contraseña de un solo uso (OTP) para un Cuenta de AWS	Escritura			

Tipos de recurso definidos por Amazon SNS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon SNS

Amazon SNS define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante las etiquetas de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso mediante las claves de etiqueta desde la solicitud	ArrayOfString
sns:Endpoint	Filtra el acceso mediante la URL, la dirección de email o el ARN de una solicitud de suscripción o una suscripción confirmada anteriormente	Cadena
sns:Protocol	Filtra el acceso mediante el valor de protocolo de una solicitud de suscripción o de una suscripción confirmada anteriormente	Cadena

Acciones, recursos y claves de condiciones para SQL Workbench AWS

AWS SQL Workbench (prefijo de servicio:`sqlworkbench`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS SQL Workbench
- Tipos de recurso definidos por AWS SQL Workbench
- Claves de condición de AWS SQL Workbench

Acciones definidas por AWS SQL Workbench

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateConnectionWithChart [solo permiso]	Concede permiso para asociar una conexión con un gráfico	Escritura	chart* connection*		
AssociateConnectionWithTab	Concede permiso para asociar una conexión con una pestaña	Escritura	connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
[solo permiso]					
AssociateNotebookWithTab [solo permiso]	Concede permiso para asociar un cuaderno con una pestaña	Escritura	notebook*		
AssociateQueryWithTab [solo permiso]	Concede permiso para asociar una consulta con una pestaña	Escritura	query*		
BatchDeleteFolder [solo permiso]	Concede permiso para eliminar carpetas en su cuenta	Escritura			
BatchGetNotebookCell [solo permiso]	Concede permiso para obtener contenido de celdas de cuadernos en su cuenta	Lectura	notebook*		
CreateAccount [solo permiso]	Otorga permiso para crear una cuenta SQLWorkbench	Escritura			
CreateChart [solo permiso]	Concede permiso para crear un nuevo gráfico guardado en su cuenta	Escritura	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConnection [solo permiso]	Concede permiso para crear una nueva conexión en su cuenta	Escritura	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFolder [solo permiso]	Concede permiso para crear una carpeta en su cuenta	Escritura			
CreateNotebook [solo permiso]	Concede permiso para crear un nuevo cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookCell [solo permiso]	Concede permiso para crear una celda de cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNotebookFromVersion [solo permiso]	Concede permiso para crear un nuevo cuaderno a partir de una versión de un cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookVersion [solo permiso]	Concede permiso para crear una versión de cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery [solo permiso]	Concede permiso para crear una nueva consulta guardada en su cuenta	Escritura	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChart [solo permiso]	Concede permiso para eliminar gráficos guardados en su cuenta	Escritura	chart*		
DeleteConnection [solo permiso]	Concede permiso para eliminar conexiones guardadas en su cuenta	Escritura	connection*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteNotebook [solo permiso]	Concede permiso para eliminar cuadernos en su cuenta	Escritura	notebook*		
DeleteNotebookCell [solo permiso]	Otorga permiso para eliminar celdas de cuadernos en su cuenta	Escritura	notebook*		
DeleteNotebookVersion [solo permiso]	Otorga permiso para eliminar celdas de cuadernos en su cuenta	Escritura	notebook*		
DeleteQCustomContext [solo permiso]	Concede permiso para eliminar el contexto personalizado a nivel de cuenta	Escritura			
DeleteSavedQuery [solo permiso]	Concede permiso para eliminar consultas guardadas en su cuenta	Escritura	query*		
DeleteSqlGenerationContext [solo permiso]	Otorga permiso para eliminar el contexto de generación de SQL	Escritura			
DeleteTab [solo permiso]	Concede permiso para eliminar una pestaña guardada en su cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DriverExecute [solo permiso]	Concede permiso para ejecutar una consulta en su clúster de Redshift	Escritura	connection*		
DuplicateNotebook [solo permiso]	Concede permiso para crear un nuevo cuaderno al duplicar uno existente en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook [solo permiso]	Concede permiso para exportar un cuaderno en su cuenta	Lectura	notebook*		
GenerateSession [solo permiso]	Concede permiso para generar una nueva sesión en su cuenta	Escritura			
GetAccountInfo [solo permiso]	Concede permiso para obtener información de la cuenta	Lectura			
GetAccountSettings [solo permiso]	Concede permiso para obtener una configuración de cuenta	Lectura			
GetAutocompletionMetadata [solo permiso]	Otorga permiso para obtener los metadatos de la estructura de la base de datos para su finalización automática	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAutocompletionResource [solo permiso]	Otorga permiso para obtener los metadatos de la información de la base de datos para su finalización automática	Lectura			
GetChart [solo permiso]	Concede permiso para obtener gráficos guardados en su cuenta	Lectura	chart*		
GetConnection [solo permiso]	Concede permiso para obtener conexiones guardadas en su cuenta	Lectura	connection*		
GetNotebook [solo permiso]	Concede permiso para obtener metadatos de cuadernos en su cuenta	Lectura	notebook*		
GetNotebookVersion [solo permiso]	Concede permiso para obtener el contenido de una versión de cuaderno en su cuenta	Lectura	notebook*		
GetQCustomContext [solo permiso]	Concede permiso para obtener el contexto personalizado a nivel de cuenta	Lectura			
GetQSqlPromptQuotas [solo permiso]	Concede permiso para obtener las cuotas máximas de peticiones de SQL generativo de Q	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQSqlRecommendations [solo permiso]	Concede permiso para obtener recomendaciones de texto a SQL	Lectura			
GetQueryExecutionHistory [solo permiso]	Concede permiso para obtener el historial de ejecución de consultas guardado en su cuenta.	Lectura			
GetSavedQuery [solo permiso]	Concede permiso para obtener consultas guardadas en su cuenta	Lectura	query*		
GetSchemaInference [solo permiso]	Concede permiso para obtener las columnas y los tipos de datos de un archivo	Lectura			
GetSqlGenerationContext [solo permiso]	Otorga permiso para obtener el contexto de generación de SQL	Lectura			
GetSqlRecommendations [solo permiso]	Concede permiso para obtener recomendaciones de texto a SQL	Lectura			
GetUserInfo [solo permiso]	Concede permiso para obtener información de usuario	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetUserWorkspaceSettings [solo permiso]	Concede permiso para obtener una configuración del espacio de trabajo en su cuenta	Lectura			
ImportNotebook [solo permiso]	Concede permiso para importar un cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListConnections [solo permiso]	Concede permiso para enumerar las conexiones guardadas en su cuenta	Enumeración			
ListDatabases [solo permiso]	Concede permiso para enumerar bases de datos del clúster de Redshift	Enumeración			
ListFiles [solo permiso]	Concede permiso para enumerar archivos y carpetas	Enumeración			
ListNotebookVersions [solo permiso]	Concede permiso para obtener metadatos de versiones de cuadernos en su cuenta	Enumeración	notebook*		
ListNotebooks [solo permiso]	Concede permiso para enumerar los cuadernos en su cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQueryExecutionHistory [solo permiso]	Concede permiso para enumerar el historial de ejecución de consultas guardado en su cuenta.	Enumeración			
ListRedshiftClusters [solo permiso]	Concede permiso para enumerar clústeres de Redshift en su cuenta	Enumeración			
ListSampleDatabases [solo permiso]	Concede permiso para enumerar bases de datos	Lectura			
ListSavedQueryVersions [solo permiso]	Concede permiso para obtener versiones de consultas guardadas en su cuenta	Enumeración	query*		
ListTabs [solo permiso]	Concede permiso para enumerar las pestañas en su cuenta	Enumeración			
ListTaggedResources [solo permiso]	Concede permiso para enumerar recursos etiquetados	Lectura			
ListTagsForResource [solo permiso]	Concede permiso para enumerar las etiquetas de un recurso sqlworkbench	Lectura	chart		
			connection		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			notebook		
			query		
PassAccountSettings [solo permiso]	Otorga permiso para proporcionar la configuración de la cuenta con la solicitud	Escritura			
PutQCustomContext [solo permiso]	Concede permiso para actualizar el contexto personalizado a nivel de cuenta	Escritura			
PutSqlGenerationContext [solo permiso]	Otorga permiso para actualizar el contexto de generación de SQL	Escritura			
PutTab [solo permiso]	Concede permiso para crear o actualizar una pestaña guardada en su cuenta	Escritura			
PutUserWorkspaceSettings [solo permiso]	Concede permiso para actualizar la configuración del espacio de trabajo en su cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RestoreNotebookVersion [solo permiso]	Concede permiso para restaurar un cuaderno de su cuenta a una versión	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [solo permiso]	Concede permiso para etiquetar un recurso sqlworkbench	Etiquetado	chart		
			connection		
			notebook		
			query		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [solo permiso]	Concede permiso para desetiquetar un recurso sqlworkbench	Etiquetado	chart		
			connection		
			notebook		
			query		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateAccountConnectionSettings [solo permiso]	Concede permiso para actualizar la configuración de conexión en toda la cuenta	Escritura			
UpdateAccountExportSettings [solo permiso]	Concede permiso para actualizar la configuración de exportación en toda la cuenta	Escritura			
UpdateAccountGeneralSettings [solo permiso]	Concede permiso para actualizar la configuración general en toda la cuenta	Escritura			
UpdateAccountQSqlSettings [solo permiso]	Concede permiso para actualizar la configuración de texto a SQL de toda la cuenta	Escritura			
UpdateChart [solo permiso]	Concede permiso para actualizar un gráfico en su cuenta	Escritura	chart*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection [solo permiso]	Concede permiso para actualizar una conexión en su cuenta	Escritura	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateFileFolder [solo permiso]	Concede permiso para mover archivos guardados en su cuenta	Escritura	chart		
			query		
UpdateFolder [solo permiso]	Concede permiso para actualizar el nombre y los detalles de una carpeta en su cuenta	Escritura			
UpdateNotebook [solo permiso]	Concede permiso para actualizar metadatos de un cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateNotebookCellContent [solo permiso]	Concede permiso para actualizar una conexión en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellLayout [solo permiso]	Concede permiso para actualizar un diseño de celda de cuaderno en su cuenta	Escritura	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateSavedQuery [solo permiso]	Concede permiso para actualizar consultas guardadas en su cuenta	Escritura	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Tipos de recurso definidos por AWS SQL Workbench

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
connection	`arn:${Partition}:sqlworkbench:${Region}:${Account}:connection/${ResourceId}`	aws:ResourceTag/${TagKey}
query	`arn:${Partition}:sqlworkbench:${Region}:${Account}:query/${ResourceId}`	aws:ResourceTag/${TagKey}
chart	`arn:${Partition}:sqlworkbench:${Region}:${Account}:chart/${ResourceId}`	aws:ResourceTag/${TagKey}
notebook	`arn:${Partition}:sqlworkbench:${Region}:${Account}:notebook/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS SQL Workbench

AWS SQL Workbench define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon SQS

Amazon SQS (prefijo de servicio: `sqs`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon SQS
- Tipos de recursos definidos por Amazon SQS
- Claves de condición de Amazon SQS

Acciones definidas por Amazon SQS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddPermission	Otorga un permiso a una cola para un principal específico	Administración de permisos	queue*		
CancelMessageMoveTask	Concede permiso para cancelar una tarea de movimiento de mensajes en curso	Escritura	queue*		
ChangeMessageVisibility	Otorga permiso para cambiar el tiempo de espera de visibilidad de un mensaje especificado en una cola por un nuevo valor	Escritura	queue*		
CreateQueue	Otorga permiso para crear una nueva cola o devuelve la dirección URL de una existente	Escritura	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMessage	Otorga permiso para eliminar el mensaje especificado de la cola especificada	Escritura	queue*		
DeleteQueue	Otorga permiso para eliminar la cola especificada por la URL de cola, independientemente de que la cola esté vacía	Escritura	queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueueAttributes	Otorga permiso para obtener los atributos de la cola especificada	Lectura	queue*		
GetQueueUrl	Otorga permiso para devolver la dirección URL de una cola existente	Lectura	queue*		
ListDeadLetterSourceQueues	Otorga permiso para devolver una lista de las colas que tienen el atributo de RedrivePolicy cola configurado como cola de letra muerta	Lectura	queue*		
ListMessageMoveTasks	Concede permiso para enumerar las tareas de movimiento de mensajes	Lectura	queue*		
ListQueueTags	Otorga permiso para enumerar las etiquetas agregadas a una cola SQS	Lectura	queue*		
ListQueues	Otorga permiso para devolver una lista de colas	Lectura			
PurgeQueue	Otorga permiso para eliminar los mensajes de una cola especificada por la URL de cola	Escritura	queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ReceiveMessage	Otorga permiso para recuperar uno o varios mensajes, con un límite máximo de 10, de la cola especificada	Lectura	queue*		
RemovePermission	Otorga permiso para revocar los permisos en la política de cola que coincidan con el parámetro Label especificado	Administración de permisos	queue*		
SendMessage	Otorga permiso para entregar un mensaje a la cola especificada	Escritura	queue*		
SetQueueAttributes	Otorga permiso para establecer el valor de uno o varios atributos de cola	Escritura	queue*		
StartMessageMoveTask	Concede permiso para iniciar una tarea de movimiento de mensajes	Escritura	queue*		
TagQueue	Otorga permiso para agregar etiquetas a la cola de SQS especificada	Etiquetado	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagQueue		Etiquetado	queue*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Otorga permiso para eliminar las etiquetas de la cola SQS especificada			aws:TagKeys	

Tipos de recursos definidos por Amazon SQS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> El ARN de la cola se utiliza solo en las políticas de permisos de IAM. En las llamadas de la API y la CLI, se utiliza la URL de la cola en su lugar.

Tipos de recurso	ARN	Claves de condición
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon SQS

Amazon SQS define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Step Functions

AWS Step Functions (prefijo de servicio:`states`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Step Functions
- Tipos de recursos definidos por AWS Step Functions
- Claves de condición para AWS Step Functions

Acciones definidas por AWS Step Functions

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateActivity	Otorga permiso para crear una actividad.	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	Otorga permiso para crear una máquina de estado.	Escritura	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachineAlias	Concede permiso para crear un alias de máquina de estado	Escritura	statemachine*		
				states:StateMachineQualifier	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteActivity	Otorga permiso para eliminar una actividad.	Write	activity*		
DeleteStateMachine	Otorga permiso para eliminar una máquina de estado.	Escritura	statemachine*		
DeleteStateMachineAlias	Concede permiso para eliminar un alias de máquina de estado	Escritura	statemachine*		
				states:StateMachineQualifier	
DeleteStateMachineVersion	Concede permiso para eliminar una versión de una máquina de estado	Escritura	statemachine*		
				states:StateMachineQualifier	
DescribeActivity	Otorga permiso para describir una actividad.	Read	activity*		
DescribeExecution	Otorga permiso para describir una ejecución.	Lectura	execution*		
			express*		
DescribeMapRun	Otorga permiso para describir la ejecución de un mapa	Lectura	maprun*		
DescribeStateMachine	Otorga permiso para describir una máquina de estado.	Lectura	statemachine*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				states:StateMachineQualifier	
DescribeStateMachineAlias	Concede permiso para describir un alias de máquina de estado	Lectura	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineForExecution	Otorga permiso para describir la máquina de estado para una ejecución.	Read	execution*		
GetActivityTask	Otorga permiso a los empleados para recuperar una tarea (con el ARN de actividad especificado) cuya ejecución se haya programado por una máquina de estado en funcionamiento.	Write	activity*		
GetExecutionHistory	Otorga permiso para devolver el historial de la ejecución especificada como una lista de eventos.	Lectura	execution*		
InvokeHTTPEndpoint [solo permiso]	Concede permiso para invocar el estado de HTTP Task	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListActivities	Concede permiso para enumerar las actividades existentes	List			
ListExecutions	Concede permiso para mostrar una lista de las ejecuciones de una máquina de estado	Enumeración	maprun*		
			statemachine*		
				states:StateMachineQualifier	
ListMapRuns	Concede permiso para enumerar las ejecuciones de mapa de una ejecución	Enumeración	execution*		
ListStateMachineAliases	Concede permiso para mostrar una lista de los alias de una máquina de estado	Enumeración	statemachine*		
				states:StateMachineQualifier	
ListStateMachineVersions	Concede permiso para enumerar las versiones de una máquina de estado	Enumeración	statemachine*		
ListStateMachines	Concede permiso para mostrar una lista de las máquinas de estado existentes	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Otorga permiso para enumerar etiquetas para un recurso de AWS Step Functions	Enumeración	activity		
			statemachine		
PublishStateMachineVersion	Concede permiso para publicar una versión de una máquina de estado	Escritura	statemachine*		
RedriveExecution	Concede permiso para redireccionar una ejecución	Escritura	execution*		
RevealSecrets [solo permiso]	Concede permiso para revelar datos confidenciales de una ejecución	Lectura			
SendTaskFailure	Otorga permiso para informar que la tarea identificada por el taskToken falló.	Write			
SendTaskHeartbeat	Otorga permiso para informar al servicio que la tarea representada por el taskToken especificado sigue avanzando.	Write			
SendTaskSuccess	Otorga permiso para informar que la tarea identificada por taskToken finalizó correctamente.	Write			
StartExecution	Otorga permiso para iniciar la ejecución de una máquina de estado.	Write	statemachine*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				states:StateMachineQualifier	
StartSyncExecution	Otorga permiso para iniciar la ejecución de una máquina de estado de Synchronous Express.	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	Otorga permiso para detener una ejecución.	Escritura	execution*		
TagResource	Otorga permiso para etiquetar un recurso de AWS Step Functions	Etiquetado	activity		
			statemachine		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestState	Concede permiso para probar una definición de máquina de estado	Escritura			states:RevealSecrets
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso de AWS Step Functions	Etiquetado	activity		
			statemachine		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
UpdateMapRun	Otorga permiso para actualizar una ejecución de mapa	Escritura	maprun*		
UpdateStateMachine	Concede permiso para actualizar una máquina de estado	Escritura	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	Concede permiso para actualizar un alias de máquina de estado	Escritura	statemachine*		
				states:StateMachineQualifier	
ValidateStateMachineDefinition	Concede permiso para validar una definición de máquina de estados	Lectura			

Tipos de recursos definidos por AWS Step Functions

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
activity	`arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}`	aws:ResourceTag/${TagKey}
execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}`	aws:ResourceTag/${TagKey}
express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}:${ExecutionId}:${ExpressId}`	
statemachine	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}`	aws:ResourceTag/${TagKey}
statemachineversion	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineVersionId}`	aws:ResourceTag/${TagKey}
statemachinealias	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineAliasName}`	aws:ResourceTag/${TagKey}
maprun	`arn:${Partition}:states:${Region}:${Account}:mapRun:${StateMachineName}/${MapRunLabel}:${MapRunId}`	

Tipos de recurso	ARN	Claves de condición
labelled execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}`	
labelled express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}/${MapRunLabel}:${ExecutionId}:${ExpressId}`	

Claves de condición para AWS Step Functions

AWS Step Functions define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString
states:HTTPEndpoint	Filtra el acceso por el punto de conexión que el estado de la tarea HTTP permite en la solicitud	Cadena

Claves de condición	Descripción	Tipo
states:HTTPMethod	Filtra el acceso por el método que el estado de la tarea HTTP permite en la solicitud	Cadena
states:StateMachineQualifier	Filtra el acceso según el calificador del ARN de una máquina de estado	ArrayOfString

Acciones, recursos y claves de condición para AWS Storage Gateway

AWS Storage Gateway (prefijo de servicio:`storagegateway`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Storage Gateway
- Tipos de recurso definidos por AWS Storage Gateway
- Claves de condición de AWS Storage Gateway

Acciones definidas por AWS Storage Gateway

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateGateway	Otorga permiso para activar la gateway implementada anteriormente en el host.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	Otorga permiso para configurar uno o varios discos locales de gateway como caché para un gateway de volumen en caché.	Write	gateway*		
AddTagsToResource	Otorga permiso para agregar una o más etiquetas al recurso especificado.	Etiquetado	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
AddUploadBuffer	Otorga permiso para configurar uno o varios discos locales de gateway como búfer de carga para una gateway determinada.	Write	gateway*		
AddWorkingStorage	Otorga permiso para configurar uno o varios discos locales de gateway como almacén de trabajo para una gateway.	Write	gateway*		
AssignTapePool	Otorga permiso para mover una cinta al grupo de destino especificado	Escritura	tape*		
			tapepool*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate FileSystem	Otorga permiso para asociar un sistema de FSx archivos de Amazon con la pasarela de FSx archivos de Amazon	Escritura	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	Otorga permiso para conectar un volumen a una conexión iSCSI y, a continuación, asocia el volumen a la gateway especificada.	Write	gateway*		
			volume*		
BypassGovernanceRetention	Otorga permiso para permitir que se omita el bloqueo de retención de gobierno en un grupo	Write	tapepool*		
CancelArchival	Otorga permiso para cancelar el archivado de una cinta virtual en la estantería de cintas virtuales (VTS) después de que se inicie el proceso de archivado.	Escritura	gateway*		
			tape*		
CancelCacheReport	Otorga permiso para cancelar un informe de caché	Escritura	cache-report*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelRetrieval	Otorga permiso para cancelar la recuperación de una cinta virtual de la estantería de cintas virtuales (VTS) en una gateway después de que se inicie el proceso de recuperación.	Write	gateway*		
			tape*		
CreateCachediSCSIVolume	Otorga permiso para crear un volumen en caché en una gateway especificada en la memoria caché. Esta operación solo se admite en la arquitectura de volúmenes en caché de gateway.	Write	gateway*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	Otorga permiso para crear un recurso compartido de archivos NFS en una gateway de archivos existente.	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	Otorga permiso para crear un recurso compartido de archivos SMB en una gateway de archivos existente.	Write	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Otorga permiso para comenzar una instantánea de un volumen.	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	Otorga permiso para comenzar una instantánea de una gateway desde un punto de recuperación de volumen.	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	Otorga permiso para crear un volumen en una gateway especificada.	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTapePool	Otorga permiso para crear un grupo de cintas.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	Otorga permiso para crear una cinta virtual con su código de barras.	Write	gateway* tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	Otorga permiso para crear una o varias cintas virtuales . Puede escribir datos en las cintas virtuales y después archivarlas.	Write	gateway* tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutomaticTapeCreationPolicy	Otorga permiso para eliminar la política de creación automática de cintas configurada en una VTL de gateway	Write	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteBandwidthRateLimit	Otorga permiso para eliminar los límites de ancho de banda de una gateway.	Escritura	gateway*		
DeleteCacheReport	Otorga permiso para eliminar los metadatos asociados a un informe de caché	Escritura	cache-report*		
DeleteChapCredentials	Otorga permiso para eliminar las credenciales del protocolo CHAP (Challenge-Handshake Authentication Protocol, Protocolo de autenticación por desafío mutuo) para un destino iSCSI y par de iniciadores especificados.	Write	target*		
DeleteFileShare	Otorga permiso para eliminar un recurso compartido de archivos de una gateway de archivos.	Write	share*		
DeleteGateway	Concede permiso para eliminar una puerta de enlace	Write	gateway*		
DeleteSnapshotSchedule	Otorga permiso para eliminar una instantánea de un volumen.	Write	volume*		
DeleteTape	Otorga permiso para eliminar la cinta virtual especificada.	Write	gateway* tape*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteTapeArchive	Otorga permiso para eliminar la cinta virtual especificada de la estantería de cintas virtuales (VTS).	Write			
DeleteTapePool	Otorga permiso para eliminar el grupo de cintas especificado.	Escritura	tapepool*		
DeleteVolume	Otorga permiso para eliminar el volumen de puerta de enlace especificado que creó anteriormente mediante la CreateStoredi SCSIVolume API CreateCachedi SCSIVolume o	Escritura	volume*		
DescribeAvailabilityMonitorTest	Otorga permiso para obtener la información acerca de la prueba de monitoreo de alta disponibilidad más reciente que se realizó en la gateway.	Read	gateway*		
DescribeBandwidthRateLimit	Otorga permiso para obtener los límites de ancho de banda de una gateway.	Read	gateway*		
DescribeBandwidthRateLimitSchedule	Otorga permiso para obtener la programación de los límites de ancho de banda de una gateway.	Read	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCache	Otorga permiso para obtener información sobre la caché de una gateway. Esta operación solo se admite en la arquitectura de volúmenes en caché de gateway.	Lectura	gateway*		
DescribeCacheReport	Otorga permiso para obtener una descripción de un informe de caché	Lectura	cache-report*		
DescribeCachediSCSIVolumes	Otorga permiso para obtener una descripción de los volúmenes de gateway especificados en la solicitud. Esta operación solo se admite en la arquitectura de volúmenes en caché de gateway.	Read	volume*		
DescribeChapCredentials	Otorga permiso para obtener una matriz de información de credenciales del protocolo de autenticación por desafío mutuo (CHAP, Challenge-Handshake Authentication Protocol) para un destino iSCSI, uno por cada par de iniciadores de destino.	Read	target*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeFileSystemAssociations	Otorga permiso para obtener una descripción de una o varias asociaciones de sistema de archivos	Read	fs-association*		
DescribeGatewayInformation	Otorga permiso para activar obtener los metadatos de una gateway; por ejemplo, su nombre, las interfaces de red, la zona horaria configurada y el estado (si la gateway se está ejecutando o no).	Read	gateway*		
DescribeMaintenanceStartTime	Otorga permiso para obtener la hora de inicio de mantenimiento semanal de la gateway, incluido el día y la hora de la semana.	Read	gateway*		
DescribeNFSFileShares	Otorga permiso para obtener una descripción de uno o más recursos compartidos de archivos de una gateway de archivos.	Read	share*		
DescribeSMBFileShares	Otorga permiso para obtener una descripción de uno o más recursos compartidos de archivos de una gateway de archivos.	Read	share*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSMBSettings	Otorga permiso para obtener una descripción de una configuración de recurso compartido de archivos de bloque de mensajes del servidor (SMB) de una gateway de archivos.	Read	gateway*		
DescribeSnapshotSchedule	Otorga permiso para describir el programa de instantáneas para el volumen de gateway especificado.	Read	volume*		
DescribeStorediSCSIVolumes	Otorga permiso para obtener la descripción de los volúmenes de gateway especificados en la solicitud.	Read	volume*		
DescribeTapeArchives	Otorga permiso para obtener una descripción de cintas virtuales especificadas en la estantería de cintas virtuales (VTS).	Read			
DescribeTapeRecoveryPoints	Otorga permiso para obtener una lista de puntos de recuperación de cintas virtuales que están disponibles para la VTL de gateway especificada.	Read	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeTapes	Otorga permiso para obtener una descripción del nombre de recurso de Amazon (ARN) especificado de las cintas virtuales.	Read	gateway*		
DescribeUploadBuffer	Otorga permiso para obtener información acerca del búfer de carga de una gateway.	Read	gateway*		
DescribeVTLDevices	Otorga permiso para obtener una descripción de los dispositivos de biblioteca de cintas virtuales (VTL) de la gateway especificada.	Read	gateway*		
DescribeWorkingStorage	Otorga permiso para obtener información acerca del almacén de trabajo de una gateway.	Read	gateway*		
DetachVolume	Otorga permiso para desconectar un volumen de una conexión iSCSI y, a continuación, separa el volumen de la gateway especificada.	Write	volume*		
DisableGateway	Otorga permiso para desactivar una gateway cuando ya no está funcionando.	Escritura	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateFileSystem	Concede permiso para desasociar un sistema de FSx archivos de Amazon de una pasarela de FSx archivos de Amazon	Escritura	fs-association*		
EvictFilesFailingUpload	Otorga permiso para limpiar la caché de un recurso compartido de entradas de archivos que no se cargan correctamente en Amazon S3	Escritura	share*		
JoinDomain	Otorga permiso para permitirle unirse a un dominio de Active Directory.	Escritura	gateway*		
ListAutomaticTapeCreationPolicies	Otorga permiso para enumerar las políticas de creación automática de cintas configuradas en la Gateway-VTL especificada o en todas las pasarelas que sean propiedad de su VTLs Cuenta de AWS	Enumeración			
ListCacheReports	Otorga permiso para obtener una lista de los informes en caché que son propiedad de su Cuenta de AWS	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListFileShares	Otorga permiso para obtener una lista de los archivos compartidos para una puerta de enlace de archivos específica, o la lista de los recursos compartidos de archivos propiedad de su Cuenta de AWS	Enumeración			
ListFileSystemAssociations	Otorga permiso para obtener una lista de las asociaciones del sistema de archivos para la gateway especificada	Enumeración			
ListGateways	Otorga permiso para enumerar las pasarelas que son propiedad de una persona Cuenta de AWS en una región especificada en la solicitud . La lista devuelta se ordena por el nombre de recurso de Amazon (ARN) de la gateway.	List			
ListLocalDisks	Otorga permiso para obtener una lista de los discos locales de la gateway.	List	gateway*		
ListTagsForResource	Otorga permiso para obtener las etiquetas que se han agregado al recurso especificado.	Enumeración	gateway		
			share		
			tape		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			volume		
ListTapePools	Otorga permiso para enumerar los grupos de cintas que sean propiedad de su Cuenta de AWS	Enumeración			
ListTapes	Otorga permiso para enumerar las cintas virtuales de la biblioteca de cintas virtuales (VTL) y la estantería de cintas virtuales (VTS).	List			
ListVolumeInitiators	Otorga permiso para enumerar los iniciadores iSCSI conectados a un volumen.	List	volume*		
ListVolumeRecoveryPoints	Otorga permiso para enumerar los puntos de recuperación de una gateway especificada.	List	gateway*		
ListVolumes	Otorga permiso para enumerar los volúmenes almacenados iSCSI de una gateway.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
NotifyWhenUploaded	Concede permiso para enviarle una notificación a través de CloudWatch Eventos cuando todos los archivos escritos en su recurso compartido de archivos NFS se hayan cargado en Amazon S3	Escritura	share*		
RefreshCache	Otorga permiso para actualizar la caché del recurso de archivos compartido.	Write	share*		
RemoveTagsFromResource	Otorga permiso para eliminar una o más etiquetas del recurso especificado.	Etiquetado	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResetCache	Otorga permiso para restablecer todos los discos de caché que han tenido un error y los deja listos para reconfiguración como almacenamiento en caché.	Write	gateway*		
RetrieveTapeArchive	Otorga permiso para recuperar una cinta virtual archivada de la estantería de cintas virtuales (VTS) de una VTL de gateway.	Write	gateway*		
			tape*		
RetrieveTapeRecoveryPoint	Otorga permiso para recuperar el punto de recuperación para la cinta virtual especificada.	Write	gateway*		
			tape*		
SetLocalConsolePassword	Otorga permiso para establecer la contraseña de la consola local de la máquina virtual.	Write	gateway*		
SetSMBGuestPassword	Otorga permiso para establecer la contraseña del usuario invitado SMB.	Write	gateway*		
ShutdownGateway	Otorga permiso para cerrar una puerta de enlace.	Write	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartAvailabilityMonitorTest	Otorga permiso para iniciar una prueba que compruebe que la gateway especificada está configurada para el monitoreo de alta disponibilidad en el entorno de host.	Escritura	gateway*		
StartCacheReport	Otorga permiso para iniciar un informe de caché para un recurso compartido de archivos existente	Escritura	share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	Otorga permiso para iniciar una gateway que había cerrado previamente.	Write	gateway*		
UpdateAutomaticTapeCreationPolicy	Otorga permiso para actualizar la política de creación automática de cintas configurada en una VTL de gateway	Write	gateway*		
			tapepool*		
UpdateBandwidthRateLimit	Otorga permiso para actualizar los límites de ancho de banda de una gateway.	Write	gateway*		
UpdateBandwidthRateLimitSchedule	Otorga permiso para actualizar la programación de los límites de ancho de banda de una gateway.	Write	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateChapCredentials	Otorga permiso para actualizar las credenciales del protocolo de autenticación por desafío mutuo (CHAP, Challenge-Handshake Authentication Protocol) para un destino iSCSI especificado.	Write	target*		
UpdateFileSystemAssociation	Otorga permiso para actualizar una asociación de sistema de archivos	Write	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	Otorga permiso para actualizar los metadatos de una gateway, que incluyen el nombre y la zona horaria de la gateway.	Write	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateGatewaySoftwareNow	Otorga permiso para actualizar el software de máquina virtual (VM) de la gateway.	Write	gateway*		
UpdateMaintenanceStartTime	Otorga permiso para actualizar la información sobre la hora de inicio de mantenimiento semanal de la gateway, incluido la hora y el día de la semana. La hora de mantenimiento es la hora de la zona horaria de la gateway.	Write	gateway*		
UpdateNFSFileShare	Otorga permiso para actualizar un recurso compartido de archivos NFS.	Write	share*		
UpdateSMBFileShare	Otorga permiso para actualizar un recurso compartido de archivos SMB.	Write	share*		
UpdateSMBFileShareVisibility	Otorga permiso para actualizar si los recursos compartidos de una gateway son visibles en una vista de red o lista de exploración.	Escritura	gateway*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSMBLocalGroups	Otorga permiso para actualizar la lista de usuarios y grupos de Active Directory que cuentan con permisos especiales para los recursos compartidos de archivos SMB en la puerta de enlace	Escritura	gateway*		
UpdateSMBSecurityStrategy	Otorga permiso para actualizar la estrategia de seguridad SMB en una gateway de archivos.	Write	gateway*		
UpdateSnapshotSchedule	Otorga permiso para actualizar un programa de instantáneas configurado para un volumen de gateway.	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	Otorga permiso para actualizar el tipo de cambiador de medios en una VTL de gateway.	Escritura	device*		

Tipos de recurso definidos por AWS Storage Gateway

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
cache-report	`arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}/cache-report/${CacheReportId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}`	
fs-association	`arn:${Partition}:storagegateway:${Region}:${Account}:fs-association/${FsaId}`	aws:ResourceTag/${TagKey}
gateway	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
share	`arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}`	aws:ResourceTag/${TagKey}
tape	`arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}`	aws:ResourceTag/${TagKey}
tapepool	`arn:${Partition}:storagegateway:${Region}:${Account}:tapepool/${PoolId}`	aws:ResourceTag/${TagKey}
target	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}`	
volume	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Storage Gateway

AWS Storage Gateway define las siguientes claves de condición que se pueden usar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Claves de condición, recursos y acciones para AWS Supply Chain

AWS La cadena de suministro (prefijo de servicio:`scn`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Supply Chain
- Tipos de recursos definidos por AWS Supply Chain
- Claves de condición para AWS Supply Chain

Acciones definidas por AWS Supply Chain

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssignAdminPermissionsToUser	Otorga permiso para añadir el permiso de administrador AWS de la cadena de suministro a un usuario federado	Escritura	instance*		
CreateBillOfMaterialsImportJob	Otorga permiso para crear BillOfMaterialsImportJob uno que importará un archivo CSV de registros BillOfMaterials	Escritura	instance*		
CreateDataIntegrationFlow	Otorga un permiso de creación DataIntegrationFlow que puede transformarse de varias fuentes a un solo destino	Escritura	instance*		
CreateDataLakeDataset	Concede permiso para crear el conjunto de datos del lago de datos	Escritura	instance*		
CreateDataLakeNamespace	Otorga permiso para crear el espacio de nombres del lago de datos	Escritura	instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateInstance	Otorga permiso para crear una nueva instancia de la AWS cadena de suministro	Escritura	instance*		
CreateSSOApplication	Otorga permiso para crear una aplicación del Centro de Identidad de IAM para una instancia AWS de cadena de suministro	Escritura	instance*		
DeleteDataIntegrationFlow	Otorga permiso para eliminar el DataIntegrationFlow	Escritura	data-integration-flow*		
DeleteDataLakeDataset	Concede permiso para eliminar el conjunto de datos del lago de datos	Escritura	dataset*		
DeleteDataLakeNamespace	Otorga permiso para eliminar el espacio de nombres del lago de datos	Escritura	namespace*		
DeleteInstance	Otorga permiso para eliminar una instancia de la AWS cadena de suministro	Escritura	instance*		
DeleteSSOApplication	Otorga permiso para eliminar la aplicación IAM Identity Center de la instancia de la cadena de AWS suministro	Escritura	instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInstance	Otorga permiso para ver los detalles de una instancia de la cadena AWS de suministro	Lectura	instance*		
GetBillOfMaterialsImportJob	Otorga permiso para ver el estado y los detalles de una BillOfMaterialsImportJob	Lectura	bill-of-materials-import-job*		
GetDataIntegrationEvent	Otorga permiso para obtener un DataIntegrationEvent	Lectura	instance*		
GetDataIntegrationFlow	Otorga permiso para obtener los DataIntegrationFlow detalles	Lectura	data-integration-flow*		
GetDataIntegrationFlowExecution	Otorga permiso para obtener una ejecución concreta de una determinada ejecución DataIntegrationFlow	Lectura	data-integration-flow*		
GetDataLakeDataset	Concede permiso para obtener los detalles del conjunto de datos	Lectura	dataset*		
GetDataLakeNamespace	Otorga permiso para obtener los detalles del espacio de nombres	Lectura	namespace*		
GetInstance	Otorga permiso para ver los detalles de una instancia de la cadena de AWS suministro	Lectura	instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListAdminUsers	Otorga permiso para incluir a los administradores de la cadena de AWS suministro de una instancia	Enumeración	instance*		
ListDataIntegrationEvents	Otorga permiso para enumerar todos los DataIntegrationEvents elementos de una instancia	Enumeración	instance*		
ListDataIntegrationFlowExecutions	Otorga permiso para enumerar todas las ejecuciones de una determinada ejecución DataIntegrationFlow	Enumeración	data-integration-flow*		
ListDataIntegrationFlows	Otorga permiso para enumerarlas todas DataIntegrationFlows de forma paginada	Enumeración	instance*		
ListDataLakeDatasets	Concede permiso para enumerar los conjuntos de datos del lago de datos bajo una instancia y un espacio de nombres específicos	Enumeración	instance*		
ListDataLakeNamespaces	Otorga permiso para enumerar los espacios de nombres de los lagos de datos en una instancia específica	Enumeración	instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListInstances	Otorga permiso para ver las instancias de la cadena de AWS suministro asociadas a una Cuenta de AWS	Enumeración	instance*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un recurso AWS de la cadena de suministro	Enumeración	instance*		
RemoveAdminPermissionsForUser	Otorga permiso para eliminar el permiso de administrador de la cadena de AWS suministro a un usuario federado	Escritura	instance*		
SendDataIntegrationEvent	Otorga permiso para crear una DataIntegrationEvent que ingiera datos en tiempo real	Escritura	instance*		
TagResource	Otorga permiso para etiquetar un recurso de la cadena AWS de suministro	Etiquetado	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso de la cadena de AWS suministro	Etiquetado	instance*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDataIntegrationFlow	Otorga permiso para actualizar el DataIntegrationFlow	Escritura	data-integration-flow*		
UpdateDataLakeDataset	Concede permiso para actualizar el conjunto de datos del lago de datos	Escritura	dataset*		
UpdateDataLakeNamespace	Otorga permiso para actualizar el espacio de nombres del lago de datos	Escritura	namespace*		
UpdateInstance	Otorga permiso para actualizar una instancia de la AWS cadena de suministro	Escritura	instance*		

Tipos de recursos definidos por AWS Supply Chain

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
instance	`arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}`	

Tipos de recurso	ARN	Claves de condición
bill-of-materials-import-job	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/bill-of-materials-import-job/${JobId}	
data-integration-flow	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/data-integration-flows/${FlowName}	
namespace	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}	
dataset	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}/datasets/${DatasetName}	

Claves de condición para AWS Supply Chain

AWS La cadena de suministro define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante los pares de clave-valor de etiqueta de la solicitud.	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso mediante los pares de clave-valor de etiqueta asociados al recurso.	Cadena
aws:TagKeys	Filtra el acceso mediante las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Support

AWS Support (prefijo de servicio:`support`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Support
- Tipos de recursos definidos por AWS Support
- Claves de condición de AWS Support

Acciones definidas por AWS Support

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Soporte ofrece la posibilidad de acceder a los casos, modificarlos y resolverlos, así como de utilizar las acciones de Trusted Advisor. Cuando utiliza la API de Support para llamar a acciones relacionadas con Trusted Advisor, ninguna de las acciones «trustedadvisor:*»

restringe el acceso. Las acciones "trustedadvisor:*" se aplican únicamente a Trusted Advisor en la AWS Management Console.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddAttachmentsToSet	Otorga permiso para añadir uno o más archivos adjuntos a un AWS Support caso	Escritura			
AddCommunicationToCase	Otorga permiso para añadir una comunicación de un cliente a un AWS Support caso	Escritura			
CreateCase	Otorga permiso para crear un AWS Support caso nuevo	Escritura			
DescribeAttachment	Concede permiso para describir los detalles de un elemento adjunto	Lectura			
DescribeCaseAttributes	Otorga permiso para permitir que los servicios secundarios lean los atributos de los AWS Support casos. Se trata de una función gestionada internamente	Lectura			
DescribeCaseOptions	Otorga permiso para describir las opciones disponibles para un solo caso. AWS Support Se trata de una función administrada internamente	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCases	Otorga permiso para enumerar AWS Support los casos que coincidan con las entradas dadas	Lectura			
DescribeCommunication	Otorga permiso para obtener una sola comunicación y los archivos adjuntos de un solo AWS Support caso	Lectura			
DescribeCommunications	Otorga permiso para enumerar las comunicaciones y los archivos adjuntos de uno o más AWS Support casos	Lectura			
DescribeCreateCaseOptions	Concede permiso para describir las opciones disponibles para crear un caso de soporte	Lectura			
DescribeIssueTypes	Otorga permiso para devolver los tipos de emisión de AWS Support los casos	Lectura			
DescribeServices	Otorga permiso para enumerar AWS los servicios y las categorías que se aplican a cada servicio	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSeverityLevels	Otorga permiso para enumerar los niveles de gravedad que se pueden asignar a un AWS Support caso	Lectura			
DescribeSupportLevel	Otorga permiso para devolver el nivel de soporte de un identificador de AWS cuenta	Lectura			
DescribeSupportedLanguages	Concede permiso para describir los idiomas de soporte disponibles para un código de categoría, un código de servicio y un tipo de error determinados	Lectura			
DescribeTrustedAdvisorCheckRefreshStatuses	Concede permiso para obtener el estado de una comprobación de actualización de Trusted Advisor basada en una lista de identificadores de comprobación	Lectura			
DescribeTrustedAdvisorCheckResult	Concede permiso para obtener los resultados de la comprobación de Trusted Advisor que tenga el identificador de comprobación especificado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeTrustedAdvisorCheckSummaries	Concede permiso para obtener los resúmenes de los resultados de las comprobaciones de Trusted Advisor que tengan los identificadores de comprobación especificados	Lectura			
DescribeTrustedAdvisorChecks	Concede permiso para obtener una lista de todas las comprobaciones disponibles de Trusted Advisor, incluidos el nombre, el identificador, la categoría y la descripción	Lectura			
GetInteraction	Otorga permiso para obtener asistencia personalizada para la solución de problemas técnicos y de cuenta para una interacción específica	Lectura			
InitiateCallForCase	Otorga permiso para iniciar una llamada en AWS Support Center. Se trata de una función administrada internamente	Escritura			
InitiateChatForCase	Otorga permiso para iniciar un chat en AWS Support Center. Se trata de una función gestionada internamente	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutCaseAttributes	Otorga permiso para permitir que los servicios secundarios adjunten atributos a AWS Support los casos. Se trata de una función administrada internamente	Escritura			
RateCaseCommunication	Otorga permiso para calificar la comunicación de AWS Support cualquier caso	Escritura			
RefreshTrustedAdvisorCheck	Concede permiso para solicitar una actualización de la comprobación de Trusted Advisor que tenga el identificador de comprobación especificado	Escritura			
ResolveCase	Otorga permiso para resolver cualquier AWS Support caso	Escritura			
SearchForCases	Otorga permiso para devolver una lista de AWS Support casos que coincide con las entradas proporcionadas	Lectura			
StartInteraction	Otorga permiso para iniciar una interacción específica a fin de recibir asistencia personalizada para la resolución de problemas técnicos y de cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateCaseSeverity	Otorga permiso para actualizar la gravedad de un solo AWS Support caso. Se trata de una función administrada internamente	Escritura			
UpdateInteraction	Concede permiso para actualizar una interacción específica a fin de recibir asistencia personalizada para la resolución de problemas técnicos y de cuenta	Escritura			

Tipos de recursos definidos por AWS Support

AWS Support no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Support, especifique `"Resource": "*"` en su política.

Claves de condición de AWS Support

Support no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Support App en Slack

AWS Support La aplicación de Slack (prefijo de servicio:`supportapp`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Support App en Slack
- Tipos de recursos definidos por AWS Support App en Slack
- Claves de condición para AWS Support App en Slack

Acciones definidas por AWS Support App en Slack

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSlackChannelConfiguration	Concede permiso para crear una configuración de canal de Slack para la cuenta	Escritura			
DeleteAccountAlias	Concede permiso para eliminar un alias de la cuenta	Escritura			
DeleteSlackChannelConfiguration	Concede permiso para eliminar una configuración de canal de Slack de la cuenta	Escritura			
DeleteSlackWorkspaceConfiguration	Concede permiso para eliminar una configuración de espacio de trabajo de Slack de la cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeSlackChannels [solo permiso]	Otorga permiso para incluir todos los canales públicos de Slack de un espacio de trabajo que hayan invitado a la aplicación AWS Support	Lectura			
GetAccountAlias	Concede permiso para obtener el alias de la cuenta	Lectura			
GetSlackOauthParameters [solo permiso]	Otorga permiso para obtener los parámetros del OAuth código de Slack, que la AWS Support aplicación utiliza para autorizar el espacio de trabajo	Lectura			
ListSlackChannelConfigurations	Concede permiso para enumerar todas las configuraciones de canales de Slack de la cuenta	Lectura			
ListSlackWorkspaceConfigurations	Concede permiso para enumerar todas las configuraciones de espacios de trabajo de Slack de la cuenta	Lectura			
PutAccountAlias	Concede permiso para crear o actualizar un alias de la cuenta	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RedeemSlackOauthCode [solo permiso]	Otorga permiso para canjear el OAuth código de Slack, que la AWS Support aplicación utiliza para autorizar el espacio de trabajo	Escritura			
RegisterSlackWorkspaceForOrganization	Otorga permiso para registrar un espacio de trabajo de Slack a una persona Cuenta de AWS que forma parte de una organización	Escritura			
UpdateSlackChannelConfiguration	Concede permiso para actualizar la configuración de un canal de Slack para la cuenta	Escritura			

Tipos de recursos definidos por AWS Support App en Slack

AWS Support La aplicación de Slack no permite especificar un ARN de recurso en `Resource` el elemento de una declaración de política de IAM. Para permitir el acceso a AWS Support App en Slack, especifique `"Resource": "*"` en la política.

Claves de condición para AWS Support App en Slack

Support App no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las declaraciones de las políticas. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Support Console

AWS Support La consola (prefijo de servicio:`support-console`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la consola de AWS Support
- Tipos de recursos definidos por la consola de AWS Support
- Claves de condición de la consola de AWS Support

Acciones definidas por la consola de AWS Support

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CheckSubscription [solo permiso]	Otorga permiso para comprobar si la cuenta tiene acceso a un producto determinado	Lectura			
CreateCaseDraft [solo permiso]	Otorga permiso para crear o actualizar un borrador de caso para el tipo de caso en cuestión	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateContact [solo permiso]	Otorga permiso para crear un contacto autenticado para el tipo de contacto dado	Escritura			
DeleteCaseDraft [solo permiso]	Otorga permiso para eliminar un borrador de caso para el tipo de caso dado	Escritura			
DescribeDynamicHelp [solo permiso]	Otorga permiso para obtener recursos de ayuda dinámicos para un servicio y una categoría determinados	Lectura			
GetAccountGovCloudEnabled [solo permiso]	Otorga permiso para determinar si la cuenta llamante está GovCloud habilitada	Lectura			
GetAccountState [solo permiso]	Otorga permiso para obtener el estado de la cuenta que realiza la llamada	Lectura			
GetBanner [solo permiso]	Otorga permiso para obtener la información del banner de soporte	Lectura			
GetCaseDraft [solo permiso]	Otorga permiso para obtener un borrador de caso para un tipo de caso determinado	Lectura			
GetQuestionnaire [solo permiso]	Otorga permiso para obtener un cuestionario de comentarios	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SaveFeedback [solo permiso]	Otorga permiso para guardar los comentarios del cuestionario	Escritura			

Tipos de recursos definidos por la consola de AWS Support

AWS Support La consola no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la consola de AWS Support , especifique `"Resource": "*"` en su política.

Claves de condición de la consola de AWS Support

Support Console no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Support Plans

AWS Support Plans (prefijo de servicio:`supportplans`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Support Plans

- Tipos de recursos definidos por AWS Support Plans
- Claves de condición de AWS Support Plans

Acciones definidas por AWS Support Plans

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateSupportPlanSchedule [solo permiso]	Concede permiso para crear cronogramas de planes de soporte para ello Cuenta de AWS	Escritura			
GetSupportPlan [solo permiso]	Otorga permiso para ver los detalles del plan de apoyo actual para este fin Cuenta de AWS	Lectura			
GetSupportPlanUpdateStatus [solo permiso]	Concede permiso para ver detalles sobre el estado de una solicitud de actualización de un plan de soporte	Lectura			
ListSupportPlanModifiers [solo permiso]	Otorga permiso para ver una lista de todos los modificadores del plan de apoyo para este propósito Cuenta de AWS	Enumeración			
StartSupportPlanUpdate [solo permiso]	Otorga permiso para actualizar el plan de soporte para ello Cuenta de AWS	Escritura			

Tipos de recursos definidos por AWS Support Plans

AWS Support Plans no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Support Plans, especifique `"Resource": "*"` en su política.

Claves de condición de AWS Support Plans

Support Plans no tiene claves de contexto específicas de servicios que se puedan usar en el elemento `Condition` de la instrucción de la política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para las Recomendaciones de AWS Support

AWS Support Las recomendaciones (prefijo de servicio:`supportrecommendations`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las Recomendaciones de AWS Support
- Tipos de recursos definidos por las Recomendaciones de AWS Support
- Claves de condición para las Recomendaciones de AWS Support

Acciones definidas por las Recomendaciones de AWS Support

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSupportTroubleshootingResponse [solo permiso]	Otorga permiso a la GetSupportTroubleshootingResponse API, que muestra las respuestas a los problemas de los usuarios	Lectura			
StartSupportTroubleshooting [solo permiso]	Otorga permiso a la StartSupportTroubleshooting API, que comienza a solucionar los problemas de los usuarios	Lectura			

Tipos de recursos definidos por las Recomendaciones de AWS Support

AWS Support Las recomendaciones no admiten la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a las Recomendaciones de AWS Support , especifique `"Resource": "*"` en la política.

Claves de condición para las Recomendaciones de AWS Support

Las Recomendaciones de soporte no tienen claves de contexto específicas del servicio que se puedan usar en el elemento `Condition` de una instrucción de política de IAM. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Sustainability

AWS La sostenibilidad (prefijo de servicio:`sustainability`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Sustainability
- Tipos de recurso definidos por AWS Sustainability
- Claves de condición de AWS Sustainability

Acciones definidas por AWS Sustainability

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCarbonFootprintSummary	Concede permiso para ver la herramienta de huella de carbono	Lectura			

Tipos de recurso definidos por AWS Sustainability

AWS La sostenibilidad no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Sustainability, especifique `"Resource": "*"` en su política.

Claves de condición de AWS Sustainability

Sustainability no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Systems Manager

AWS Systems Manager (prefijo de servicio:`ssm`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Systems Manager
- Tipos de recursos definidos por AWS Systems Manager
- Claves de condición para AWS Systems Manager

Acciones definidas por AWS Systems Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AddTagsToResource	Otorga permiso para agregar o sobrescribir una o más etiquetas para un recurso específico AWS	Etiquetado	association		
			automation-execution		
			document		
			instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
AssociateOpsItemRelatedItem	Otorga permiso para asociarse RelatedItem a un OpsItem	Escritura	opsitem*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelCommand	Concede permiso para cancelar un comando «Ejecutar comando» especificado	Write			
CancelMaintenanceWindowExecution	Concede permiso para cancelar la ejecución de un periodo de mantenimiento en curso	Escritura	maintenancewindow*		
CreateActivation	Otorga permiso para crear una activación que se utiliza para registrar servidores y máquinas virtuales locales (VMs) con Systems Manager	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociation	Concede permiso para asociar un documento de Systems Manager especificado con instancias u otros destinos especificados	Escritura	association*		
			document*		
			instance		
			managed-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociationBatch	Otorga permiso para combinar entradas para varias CreateAssociation operaciones en un solo comando	Escritura	document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocument	Concede permiso para crear un documento SSM de Systems Manager	Write	document*		iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys ssm:DocumentType	
CreateMaintenanceWindow	Concede permiso para crear un periodo de mantenimiento	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsItem	Otorga permiso para crear una OpsItem entrada OpsCenter	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsMetadata	Otorga permiso para crear un OpsMetadata objeto para un AWS recurso	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreatePatchBaseline	Concede permiso para crear una base de referencia de parches	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDataSync	Concede permiso para crear una configuración de sincronización de datos de recursos, que recopila regularmente datos de inventario de instancias administradas y actualiza los datos en un bucket de Amazon S3	Write	resourcedatasync*		
				ssm:SyncType	
DeleteActivation	Concede permiso para eliminar una activación especificada para instancias administradas	Write			
DeleteAssociation	Concede permiso para desvincular un documento SSM especificado de una instancia especificada	Write	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteDocument	Concede permiso para eliminar un documento SSM especificado y sus asociaciones de instancia	Write	document*		
				ssm:DocumentType	
DeleteInventory	Concede permiso para eliminar un tipo de inventario personalizado especificado, o los datos asociados con un tipo de inventario personalizado.	Write			
DeleteMaintenanceWindow	Concede permiso para eliminar un periodo de mantenimiento especificado	Escritura	maintenancewindow*		
DeleteOpsItem	Otorga permiso para eliminar un OpsItem	Escritura	opsitem*		
DeleteOpsMetadata	Otorga permiso para eliminar un OpsMetadata objeto	Escritura	opsmetadata*		
DeleteParameter	Concede permiso para eliminar un parámetro SSM especificado	Write	parameter*		
				aws:ResourceTag/${TagKey}	
DeleteParameters	Concede permiso para eliminar varios parámetros SSM especificados	Write	parameter*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeletePatchBaseline	Concede permiso para eliminar una base de referencia de parches especificada	Write	patchbaseline*		
DeleteResourceDataSync	Concede permiso para eliminar una sincronización de datos de recursos especificada	Escritura	resourcedatasync*		
				ssm:SyncType	
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos de Systems Manager	Administración de permisos	document		
			opsitemgroup		
			parameter		
DeregisterManagedInstance	Concede permiso para anular el registro de un servidor local o de una máquina virtual (VM) especificados de Systems Manager	Write	managed-instance*		
				ssm:resourceTag/tag-key	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeregisterPatchBaselineForPatchGroup	Concede permiso para anular el registro de una base de referencia de parches especificada para que no sea la base de referencia de parches predeterminada para un grupo de parches especificado	Write	patchbaseline*		
DeregisterTargetFromMaintenanceWindow	Concede permiso para anular el registro de un destino especificado de un periodo de mantenimiento	Write	maintenancewindow*		
			windowtarget*		
DeregisterTaskFromMaintenanceWindow	Concede permiso para anular el registro de una tarea especificada desde un periodo de mantenimiento	Write	maintenancewindow*		
			windowtask*		
DescribeActivations	Concede permiso para ver detalles sobre una activación de instancia administrada especificada, como cuándo se creó y la cantidad de instancias registradas mediante la activación	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAssociation	Concede permiso para ver los detalles sobre la asociación especificada para una instancia o destino especificados	Read	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutionTargets	Concede permiso para ver información sobre una ejecución de una asociación especificada	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutions	Concede permiso para ver todas las ejecuciones de una asociación especificada	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeAutomationExecutions	Concede permiso para ver los detalles de todas las ejecuciones de Automation activas y terminadas	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAutomationStepExecutions	Concede permiso para ver información acerca de todas las ejecuciones de pasos activas y terminadas en un flujo de trabajo de Automation	Read	automation-execution*		
DescribeAvailablePatches	Concede permiso para ver todos los parches aptos para ser incluidos en una base de referencia de parches	Read			
DescribeDocument	Concede permiso para ver los detalles sobre un documento SSM especificado	Read	document*		
				ssm:DocumentType	
DescribeDocumentParameters	Concede permiso para mostrar información sobre los parámetros del documento SSM en la consola de Systems Manager (acción interna de Systems Manager)	Read	document*		
DescribeDocumentPermission	Concede permiso para ver los permisos de un documento SSM especificado	Read	document*		
				ssm:DocumentType	
DescribeEffectiveInstanceAssociations	Concede permiso para ver todas las asociaciones actuales de una instancia especificada	Read	instance*		
			managed-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DescribeEffectivePatchesForPatchBaseline	Concede permiso para ver detalles sobre los parches asociados actualmente con la base de referencia de parches especificada (solo Windows)	Read	patchbaseline*		
DescribeInstanceAssociationsStatus	Concede permiso para ver el estado de las asociaciones de una instancia especificada	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeInstanceInformation	Concede permiso para ver los detalles de una instancia especificada	Read			
DescribeInstancePatchStates	Concede permiso para ver lo detalles de estado sobre los parches de una instancia especificada	Read	instance*		
			managed-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstancePatchStatesForPatchGroup	Concede permiso para describir el estado de los parches en general para las instancias del grupo de parches especificado	Read			
DescribeInstancePatches	Concede permiso para ver detalles generales sobre los parches en una instancia especificada	Lectura	instance* managed-instance*		
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstanceProperties	Concede permiso a la EC2 consola Amazon del usuario para renderizar los nodos de las instancias gestionadas	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInventoryDeletions	Concede permiso para ver detalles sobre una eliminación de inventario especificada	Read			
DescribeMaintenanceWindowExecutionTaskInvocations	Concede permiso para ver detalles de la ejecución de una tarea especificada para un periodo de mantenimiento	List			
DescribeMaintenanceWindowExecutionTasks	Concede permiso para ver detalles sobre las tareas que se ejecutaron durante la ejecución de un periodo de mantenimiento especificado	List			
DescribeMaintenanceWindowExecutions	Concede permiso para ver las ejecuciones de un periodo de mantenimiento especificado	List	maintenancewindow*		
DescribeMaintenanceWindowSchedule	Concede permiso para ver detalles sobre las próximas ejecuciones de un periodo de mantenimiento especificado	List			
DescribeMaintenanceWindowTargets	Concede permiso para ver una lista de los destinos asociados a un periodo de mantenimiento especificado	List	maintenancewindow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeMaintenanceWindowTasks	Concede permiso para ver una lista de las tareas asociadas a un periodo de mantenimiento especificado	List	maintenancewindow*		
DescribeMaintenanceWindows	Concede permiso para ver información sobre todos los periodos de mantenimiento o sobre los especificados	List			
DescribeMaintenanceWindowsForTarget	Concede permiso para ver la información sobre los destinos del periodo de mantenimiento y las tareas asociadas a una instancia especificada	Enumeración			
DescribeOpsItems	Otorga permiso para ver los detalles de las especificadas OpsItems	Lectura			
DescribeParameters	Concede permiso para ver los detalles sobre un parámetro SSM especificado	List			
DescribePatchBaselines	Concede permiso para ver la información sobre las bases de referencia de parches que cumplen los criterios especificados	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribePatchGroupState	Concede permiso para ver los detalles de estado agregados de parches para un grupo de parches especificado	Enumeración			
DescribePatchGroups	Concede permiso para ver la información sobre la base de referencia de parches para un grupo de parches especificado	List			
DescribePatchProperties	Concede permiso para ver los detalles de las revisiones disponibles para un sistema operativo y una propiedad de parche especificados	List			
DescribeSessions	Concede permiso para ver una lista de sesiones recientes del Administrador de sesiones que cumplen los criterios de búsqueda especificados	Enumeración			
DisassociateOpsItemRelatedItem	Otorga permiso para desasociarse RelatedItem de un OpsItem	Escritura	opsitem*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ExecuteAPI	Otorga permiso a un administrador delegado de Systems Manager para ver los detalles OpsItems de los recursos relacionados en varias AWS cuentas del AWS Management Console	Lectura			
GetAccessToken	Otorga permiso para devolver un conjunto de credenciales para usarlo con el acceso al just-in-time nodo	Lectura	opsitem*		
GetAutomationExecution	Concede permiso para ver los detalles de una ejecución de Automation especificada	Lectura	automation-execution*		
				aws:ResourceTag/${TagKey}	
GetCalendar [solo permiso]	Concede permiso para ver detalles de un calendario específico	Lectura	document*		
GetCalendarState	Concede permiso para ver el estado de un calendario de cambios o una lista de calendarios de cambios.	Read	document*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCommandInvocation	Concede permiso para ver los detalles sobre la ejecución del comando de una invocación o complemento especificados	Read			
GetConnectionStatus	Concede permiso para ver el estado de conexión del Administrador de sesiones para una instancia administrada especificada	Read	instance		
			managed-instance		
			task		
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetDefaultPatchBaseline	Concede permiso para ver la base de referencia de parches predeterminada actual para un tipo de sistema operativo especificado	Read	patchbaseline*		
GetDeployablePatchSnapshotForInstance	Concede permiso para recuperar la instantánea de base de referencia de parches actual para una instancia especificada	Read			
GetDocument		Lectura	document*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	Concede permiso para ver el contenido de un documento SSM especificado			ssm:DocumentCategories ssm:DocumentType	
GetExecutionPreview	Otorga permiso para recuperar una vista previa existente que muestra los efectos que la ejecución de un manual de automatización específico tendría en los recursos de destino	Lectura			
GetInventory	Concede permiso para ver los detalles del inventario de instancias según los criterios especificados	Read			
GetInventorySchema	Concede permiso para ver una lista de tipos de inventario o nombres de atributos para un tipo de producto del inventario especificado	Read			
GetMaintenanceWindow	Concede permiso para ver los detalles sobre un periodo de mantenimiento especificado	Read	maintenancewindow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMaintenanceWindowExecution	Concede permiso para ver detalles sobre la ejecución de un periodo de mantenimiento especificado	Read			
GetMaintenanceWindowExecutionTask	Concede permiso para ver los detalles sobre una tarea de ejecución de un periodo de mantenimiento especificada	Read			
GetMaintenanceWindowExecutionTaskInvocation	Concede permiso para ver los detalles sobre una tarea de un periodo de mantenimiento específica que se ejecuta en un destino específico	Read			
GetMaintenanceWindowTask	Concede permiso para ver los detalles sobre las tareas registradas con un periodo de mantenimiento especificado	Lectura	maintenancewindow*		
GetManifest [solo permiso]	Concede permiso a Systems Manager y SSM Agent para determinar los requisitos de instalación de paquetes para una instancia (llamada interna de Systems Manager).	Lectura			
GetOpsItem	Otorga permiso para ver información sobre un objeto especificado OpsItem	Lectura	opsitem*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetOpsMetadata	Otorga permiso para recuperar un OpsMetadata objeto	Lectura	opsmetadata*		
GetOpsSummary	Otorga permiso para ver información resumida sobre la OpsItems base de filtros y agregadores específicos	Lectura	resourcedatasync*		
GetParameter	Concede permiso para ver la información sobre un parámetro especificado	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameterHistory	Concede permiso para ver los detalles y cambios de un parámetro especificado	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameters	Concede permiso para ver la información sobre varios parámetros especificados	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParametersByPath	Concede permiso para ver la información sobre los parámetros de una jerarquía especificada	Read	parameter*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ssm:Recursive	
GetPatchBaseline	Concede permiso para ver la información sobre una base de referencia de parches especificada	Read	patchbaseline*		
GetPatchBaselineForPatchGroup	Concede permiso para ver el ID de la base de referencia de parches actual para un grupo de parches especificado	Lectura			
GetResourcePolicies	Concede permiso para recuperar las listas de las políticas de recursos de Systems Manager	Enumeración	document		
			opsitemgroup		
			parameter		
GetServiceSetting	Otorga permiso para ver la configuración a nivel de cuenta de un servicio AWS	Lectura	servicesetting*		
LabelParameterVersion	Concede permiso para aplicar una etiqueta de identificación a una versión especificada de un parámetro	Write	parameter*		
				aws:ResourceTag/${TagKey}	
ListAssociationVersions	Concede permiso para enumerar versiones de la asociación especificada	List	association*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ListAssociations	Concede permiso para enumerar las asociaciones de un documento SSM específico o una instancia administrada	List			
ListCommandInvocations	Concede permiso para enumerar información sobre las invocaciones de comandos enviadas a una instancia especificada	Enumeración			
ListCommands	Concede permiso para enumerar los comandos enviados a una instancia especificada	Enumeración			
ListComplianceItems	Concede permiso para enumerar el estado de cumplimiento de los tipos de recursos especificados en un recurso especificado	List			
ListComplianceSummaries	Concede permiso para enumerar un recuento de resumen de recursos compatibles y no compatibles con un tipo de cumplimiento especificado	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDocumentMetadataHistory	Concede permiso para ver el historial de metadatos sobre un documento SSM especificado.	Enumeración	document*		
				ssm:DocumentType	
ListDocumentVersions	Concede permiso para enumerar todas las versiones de un documento especificado	List	document*		
				ssm:DocumentType	
ListDocuments	Concede permiso para ver la información sobre un documento SSM especificado	Enumeración			
ListInstanceAssociations	Concede permiso a SSM Agent para comprobar si hay nuevas asociaciones de State Manager (llamada interna de Systems Manager)	Enumeración	instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
ListInventoryEntries	Concede permiso para ver una lista de tipos de inventario especificados para una instancia especificada	Enumeración			
ListNodes	Otorga permiso para ver los detalles de los nodos gestionados en función de filtros específicos	Enumeración	resourcedatasync*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListNodesSummary	Otorga permiso para ver información resumida sobre los nodos gestionados en función de los filtros y agregadores especificados	Enumeración	resourcedatasync*		
ListOpsItemEvents	Otorga permiso para ver detalles sobre OpsItemEvents	Enumeración			
ListOpsItemRelatedItems	Otorga permiso para ver detalles sobre OpsItem RelatedItems	Enumeración			
ListOpsMetadata	Otorga permiso para ver una lista de OpsMetadata objetos	Enumeración			
ListResourceComplianceSummaries	Concede permiso para enumerar el recuento de resumen de nivel de recursos	List			
ListResourceDataSync	Concede permiso para enumerar la información sobre las configuraciones de sincronización de datos de recursos en una cuenta	List		ssm:SyncType	
ListTagsForResource	Concede permiso para ver una lista de etiquetas de recurso para un recurso especificado	Enumeración	association		
			automation-execution		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			document		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
				aws:ResourceTag/${TagKey}	
ModifyDocumentPermission	Otorga permiso para compartir un documento SSM personalizado de forma pública o privada con cuentas específicas AWS	Administración de permisos	document*		
				ssm:DocumentType	
PutCalendar [solo permiso]	Otorga permiso a create/edit un calendario específico	Escritura	document*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutComplianceItems	Concede permiso para registrar un tipo de conformidad y otros detalles de conformidad en un recurso especificado	Escritura	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
PutConfigurePackageResult [solo permiso]	Concede permiso a SSM Agent para generar un informe de los resultados de solicitudes específicas del agente (llamada interna de Systems Manager)	Lectura			
PutInventory	Concede permiso para agregar o actualizar productos del inventario en varias instancias administradas especificadas	Write		ssm:InventoryTypeName	
PutParameter	Concede permiso para crear un parámetro SSM	Escritura	parameter *		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys ssm:Overwrite ssm:Policies	
PutResourcePolicy	Concede permiso para crear o actualizar una política de recursos de Systems Manager	Administración de permisos	document		
			opsitemgroup		
			parameter		
RegisterDefaultPatchBaseline	Concede permiso para especificar la base de referencia de parches predeterminada para un tipo de sistema operativo	Escritura	patchbaseline*		
RegisterManagedInstance	Concede permiso para registrar un Systems Manager Agent.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
RegisterPatchBaselineForPatchGroup	Concede permiso para especificar la base de referencia de parches predeterminada para un grupo de parches especificado	Write	patchbaseline*		
RegisterTargetWithMaintenanceWindow	Concede permiso para registrar un destino con un periodo de mantenimiento especificado	Write	maintenancewindow*		
RegisterTaskWithMaintenanceWindow	Concede permiso para registrar una tarea con un periodo de mantenimiento especificado	Write	maintenancewindow*		
RemoveTagsFromResource	Concede permiso para quitar una clave de etiqueta especificada de un recurso especificado	Etiquetado	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ResetServiceSetting	Otorga permiso para restablecer la configuración del servicio de an Cuenta de AWS al valor predeterminado	Escritura	servicesetting*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResumeSession	Concede permiso para volver a conectar una sesión del Administrador de sesiones a una instancia administrada	Write	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
SendAutomationSignal	Concede permiso para enviar una señal para cambiar el comportamiento o el estado actual de una ejecución de Automation especificada.	Write	automation-execution*		
				aws:ResourceTag/${TagKey}	
SendCommand	Concede permiso para ejecutar comandos en una o más instancias administradas especificadas	Escritura	document*		
			bucket		
			instance		
			managed-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
StartAccessRequest	Otorga permiso para iniciar el flujo de trabajo para las sesiones de acceso a los just-in-time nodos	Escritura	instance		
			managed-instance		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAssociationsOnce	Concede permiso para ejecutar manualmente una asociación especificada	Write	association*		
				aws:ResourceTag/${TagKey}	
StartAutomationExecution	Concede permiso para iniciar la ejecución de un documento de Automation	Write	automation-definition*		
			document*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
StartChangeRequestExecution	Concede permiso para iniciar la ejecución de un documento de plantilla de cambio de automatización.	Escritura	automation-definition*		
			document*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:AutoApprove	
StartExecutionPreview	Otorga permiso para crear una vista previa que muestre los efectos que la ejecución de un manual de automatización específico tendría en los recursos de destino	Lectura			
StartSession	Concede permiso para iniciar una conexión a un destino especificado para una sesión del Administrador de sesiones	Write	document		
			instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			managed-instance		
			task		
				ssm:SessionDocumentAccessCheck ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey} ssm:AccessRequestId	
StopAutomationExecution	Concede permiso para detener una ejecución de automatización especificada que ya está en curso	Write	automation-execution*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TerminateSession	Concede permiso para finalizar permanentemente una conexión del Administrador de sesiones a una instancia.	Escritura	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
UnlabelParameterVersion	Concede permiso para eliminar una etiqueta de identificación de una versión especificada de un parámetro	Escritura	parameter*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	Concede permiso para actualizar una asociación y ejecutarla inmediatamente en los destinos especificados	Write	association*		
			document		
			instance		
			managed-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateAssociationStatus	Concede permiso para actualizar el estado del documento SSM asociado a una instancia especificada	Write	document*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateDocument	Concede permiso para actualizar uno o más valores para un documento SSM	Write	document*		
				ssm:DocumentType	
UpdateDocumentDefaultVersion	Concede permiso para cambiar la versión predeterminada de un documento SSM	Write	document*		
				ssm:DocumentType	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateDocumentMetadata	Concede permiso para actualizar los metadatos de un documento SSM.	Escritura	document*		
				ssm:DocumentType	
UpdateInstanceAssociationStatus [solo permiso]	Concede permiso a SSM Agent para actualizar el estado de la asociación que se está ejecutando actualmente (llamada interna de Systems Manager).	Escritura	association*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateInstanceInformation	Concede permiso a SSM Agent para enviar una señal de latido al servicio Systems Manager en la nube.	Escritura	instance		
			managed-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
UpdateMaintenanceWindow	Concede permiso para actualizar un periodo de mantenimiento especificado	Write	maintenancewindow*		
UpdateMaintenanceWindowTarget	Concede permiso para actualizar un destino de periodo de mantenimiento especificado	Write	maintenancewindow*		
			windowtarget*		
UpdateMaintenanceWindowTask	Concede permiso para actualizar una tarea de periodo de mantenimiento especificada	Write	maintenancewindow*		
			windowtask*		
UpdateManagedInstanceRole	Concede permiso para asignar o cambiar el rol de IAM asignado a una instancia administrada especificada	Escritura	iam-role*		
			managed-instance*		
				ssm:resourceTag/tag-key	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateOpsItem	Otorga permiso para editar o cambiar un OpsItem	Escritura	opsitem*		
UpdateOpsMetadata	Otorga permiso para actualizar un OpsMetadata objeto	Escritura	opsmetadata*		
UpdatePatchBaseline	Concede permiso para actualizar una base de referencia de parches especificada	Write	patchbaseline*		
UpdateResourceDataSync	Concede permiso para actualizar una definición de datos de recursos	Escritura	resourcedatasync*		
				ssm:SyncType	
UpdateServiceSetting	Otorga permiso para actualizar la configuración del servicio de un Cuenta de AWS	Escritura	servicesetting*		

Tipos de recursos definidos por AWS Systems Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> Algunos parámetros de la API de Administrador de estados han quedado obsoletos. Esto podría generar un comportamiento inesperado. Para obtener más información, consulte Trabajo con asociaciones mediante IAM.

Tipos de recurso	ARN	Claves de condición
association	`arn:${Partition}:ssm:${Region}:${Account}:association/${AssociationId}`	aws:ResourceTag/${TagKey}
automation-execution	`arn:${Partition}:ssm:${Region}:${Account}:automation-execution/${AutomationExecutionId}`	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
automation-definition	`arn:${Partition}:ssm:${Region}:${Account}:automation-definition/${AutomationDefinitionName}:${VersionId}`	
bucket	`arn:${Partition}:s3:::${BucketName}`	
document	`arn:${Partition}:ssm:${Region}:${Account}:document/${DocumentName}`	aws:ResourceTag/${TagKey} ssm:DocumentCategories ssm:DocumentType ssm:resourceTag/${TagKey}
iam-role	`arn:${Partition}:iam::${Account}:role/${RoleName}`	

Tipos de recurso	ARN	Claves de condición
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}
maintenancewindow	arn:${Partition}:ssm:${Region}:${Account}:maintenancewindow/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance	arn:${Partition}:ssm:${Region}:${Account}:managed-instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance-inventory	arn:${Partition}:ssm:${Region}:${Account}:managed-instance-inventory/${InstanceId}	
opsitem	arn:${Partition}:ssm:${Region}:${Account}:opsitem/${ResourceId}	aws:ResourceTag/${TagKey}
opsitemgroup	arn:${Partition}:ssm:${Region}:${Account}:opsitemgroup/default	
opsmetadata	arn:${Partition}:ssm:${Region}:${Account}:opsmetadata/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
patchbaseline	arn:${Partition}:ssm:${Region}:${Account}:patchbaseline/${PatchBaselineIdResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
session	arn:${Partition}:ssm:${Region}:${Account}:session/${SessionId}	ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id
resourcedatasync	arn:${Partition}:ssm:${Region}:${Account}:resource-data-sync/${SyncName}	
servicesetting	arn:${Partition}:ssm:${Region}:${Account}:servicesetting/${ResourceId}	
windowtarget	arn:${Partition}:ssm:${Region}:${Account}:windowtarget/${WindowTargetId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
windowtask	arn:${Partition}:ssm:${Region}:${Account}:windowtask/${WindowTaskId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

Tipos de recurso	ARN	Claves de condición
task	`arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Systems Manager

AWS Systems Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso a las solicitudes de “Crear” en función del conjunto de valores permitidos para las etiquetas especificadas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso en función de un par clave-valor de etiqueta asignado al recurso AWS	Cadena
aws:TagKeys	Filtra el acceso a las solicitudes 'Crear' en función de si las etiquetas obligatorias están incluidas en la solicitud.	ArrayOfString
ec2:SourceInstanceARN	Filtra acceso por ARN de la instancia en la que se originó la solicitud	ARN
ssm:AccessRequestId	Filtra el acceso verificando que un usuario tenga acceso al ID de solicitud de acceso especificado en la solicitud	Cadena
ssm:AutoApprove	Filtra el acceso al verificar que un usuario tenga permiso para iniciar flujos de trabajo de Change Manager sin un	Bool

Claves de condición	Descripción	Tipo
	paso de revisión (excepto los eventos de congelación de cambios)	
ssm:DocumentCategories	Filtra el acceso verificando que un usuario tenga permiso para acceder a un documento perteneciente a una categoría específica	ArrayOfString
ssm:DocumentType	Filtra el acceso comprobando que un usuario tiene permiso para acceder a un documento que pertenece a un tipo de documento específico. Solo está disponible en las particiones «aws», «aws-cn» y "» aws-us-gov	Cadena
ssm:InventoryTypeName	Filtra el acceso verificando que un usuario también tenga acceso a lo InventoryType especificado en la solicitud	ArrayOfString
ssm:Overwrite	Filtra el acceso al controlar si se pueden sobrescribir los parámetros de Systems Manager	Cadena
ssm:Policies	Para filtrar el acceso, controla si una entidad de IAM (usuario o rol) puede crear o actualizar un parámetro que incluya una política de parámetros	Cadena
ssm:Recursive	Filtra el acceso mediante los parámetros de Systems Manager creados en una estructura jerárquica	Cadena
ssm:SessionDocumentAccessCheck	Filtra el acceso mediante la verificación de permiso de un usuario al documento de configuración predeterminado de administración de sesión o al documento de configuración personalizado especificado en una solicitud.	Bool
ssm:SourceInstanceARN	Filtra el acceso verificando el nombre de recurso de Amazon (ARN) de AWS la instancia gestionada por el administrador de sistemas desde la que se realiza la solicitud. Esta clave no está presente cuando la solicitud proviene de la instancia gestionada autenticada con un rol de IAM asociado al perfil de la instancia EC2	ARN

Claves de condición	Descripción	Tipo
ssm:SyncType	Filtra el acceso verificando que un usuario también tenga acceso a lo ResourceDataSync SyncType especificado en la solicitud	Cadena
ssm:resourceTag/${TagKey}	Filtra el acceso mediante un par clave-valor de etiquetas asignado al recurso de Systems Manager.	Cadena
ssm:resourceTag/aws:ssmmessages:session-id	Filtra el acceso según un par clave-valor de etiqueta asignado al recurso de sesión de Systems Manager	Cadena
ssm:resourceTag/aws:ssmmessages:target-id	Filtra el acceso según un par clave-valor de etiqueta asignado al recurso de sesión de Systems Manager	Cadena
ssm:resourceTag/tag-key	Filtra el acceso mediante un par clave-valor de etiquetas asignado al recurso de Systems Manager.	Cadena

Acciones, recursos y claves de condición para AWS Systems Manager para SAP

AWS Systems Manager for SAP (prefijo de servicio:`ssm-sap`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Systems Manager para SAP
- Tipos de recursos definidos por AWS Systems Manager para SAP
- Claves de condición para AWS Systems Manager para SAP

Acciones definidas por AWS Systems Manager para SAP

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BackupDatabase	Otorga permiso para realizar operaciones de copia de seguridad en una base de datos especificada	Escritura			
DeleteResourcePermission	Otorga permiso para eliminar los permisos de recursos de nivel de SSM para SAP asociados a un recurso de base de datos de SSM para SAP	Escritura			
DeregisterApplication	Otorga permiso para dar de baja una aplicación SAP con SSM para SAP	Escritura	application		
GetApplication	Otorga permiso para acceder a información sobre una aplicación registrada en SSM para SAP al proporcionar el ID	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	de la aplicación o el ARN de la aplicación				
GetComponent	Otorga permiso para acceder a información sobre un componente registrado en SSM para SAP al proporcionar el ID de la aplicación y el ID del componente	Lectura	component		
GetDatabase	Otorga permiso para acceder a información sobre una base de datos registrada con SSM para SAP al proporcionar el ID de la aplicación, el ID del componente y el ID de la base de datos	Lectura			
GetOperation	Otorga permiso para acceder a información sobre una operación al proporcionar su ID de operación	Lectura			
GetResourcePermission	Otorga permiso para obtener los permisos de recursos de nivel de SSM para SAP asociados a un recurso de base de datos de SSM para SAP	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListApplications	Otorga permiso para recuperar una lista de todas las aplicaciones registradas en SSM for SAP bajo el nombre del cliente Cuenta de AWS	Enumeración			
ListComponents	Otorga permiso para enumerar todos los componentes de la cuenta del cliente o de una aplicación específica	Enumeración	application		
ListDatabases	Otorga permiso para enumerar todas las bases de datos de la cuenta del cliente o de una aplicación específica	Enumeración			
ListOperationEvents	Concede permiso para recuperar una lista de todos los eventos de operación en una operación especificada	Enumeración			
ListOperations	Otorga permiso para enumerar todas las operaciones de la cuenta del cliente. Se pueden aplicar filtros adicionales	Enumeración			
ListTagsForResource	Otorga permiso para enumerar las etiquetas de un ARN de recurso especificado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutResourcePermission	Otorga permiso para agregar los permisos de recursos de nivel de SSM para SAP asociados a un recurso de base de datos de SSM para SAP	Escritura			
RegisterApplication	Otorga permiso para registrar una aplicación SAP con SSM para SAP	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
RestoreDatabase	Otorga permiso para restaurar una base de datos desde otra base de datos	Escritura			
StartApplication	Concede permiso para iniciar un SSM registrado para la aplicación SAP	Escritura	application		
StartApplicationRefresh	Otorga permiso para iniciar un descubrimiento bajo demanda de una aplicación SSM registrada para SAP	Escritura	application		
StopApplication	Concede permiso para detener un SSM registrado para la aplicación SAP	Escritura	application		
TagResource	Otorga permiso para etiquetar un ARN de recurso especificado	Etiquetado	application		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			component		
			database		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Otorga permisos para eliminar las etiquetas de un ARN de recurso especificado	Etiquetado	application		
			component		
			database		
				aws:TagKeys	
UpdateApplicationSettings	Otorga permiso para actualizar la configuración de una aplicación de SSM para SAP registrada	Escritura	application		
UpdateHANABackupSettings	Otorga permiso para actualizar la configuración de copia de seguridad de HANA de una base de datos especificada	Escritura			

Tipos de recursos definidos por AWS Systems Manager para SAP

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
application	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/COMPONENT/${ComponentId}`	aws:ResourceTag/${TagKey}
database	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/DB/${DatabaseId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Systems Manager para SAP

AWS Systems Manager for SAP define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Systems Manager GUI Connect

AWS La GUI Connect de Systems Manager (prefijo de servicio:`ssm-guiconnect`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Systems Manager GUI Connect
- Tipos de recursos definidos por AWS Systems Manager GUI Connect
- Claves de condición para AWS Systems Manager GUI Connect

Acciones definidas por AWS Systems Manager GUI Connect

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelConnection [solo permiso]	Concede permiso para terminar una conexión de GUI Connect	Escritura			
DeleteConnectionRecordingPreferences	Otorga permiso para eliminar las preferencias de grabación de la conexión GUI Connect	Escritura			
GetConnection [solo permiso]	Concede permiso para obtener los metadatos de una conexión de GUI Connect	Lectura			
GetConnectionRecordingPreferences	Otorga permiso para obtener las preferencias de grabación de la conexión GUI Connect	Lectura			
ListConnections [solo permiso]	Concede permiso para enumerar los metadatos para las conexiones de GUI Connect	Enumeración			
StartConnection [solo permiso]	Concede permiso para iniciar una conexión de GUI Connect	Escritura			
UpdateConnectionRe	Otorga permiso para actualizar las preferencias de	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
cordingPreferences	grabación de la conexión GUI Connect				

Tipos de recursos definidos por AWS Systems Manager GUI Connect

AWS La GUI Connect de Systems Manager no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir que obtenga acceso a AWS Systems Manager GUI Connect, especifique`"Resource": "*"`en su política.

Claves de condición para AWS Systems Manager GUI Connect

GUI Connect no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager (prefijo de servicio:`ssm-incidents`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Systems Manager Incident Manager

- Tipos de recursos definidos por AWS Systems Manager Incident Manager
- Claves de condición para AWS Systems Manager Incident Manager

Acciones definidas por AWS Systems Manager Incident Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetIncidentFindings	Concede permiso para recuperar los detalles sobre resultados específicos para un registro de incidentes	Lectura	incident-record*		
			response-plan*		
CreateReplicationSet	Otorga permiso para crear un conjunto de reproducción	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole ssm-incidents:TagResource
CreateResponsePlan	Otorga permiso para crear un plan de respuesta	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole ssm-incidents:TagResource
CreateTimelineEvent	Otorga permiso con el fin de crear un evento de línea de tiempo para un registro de incidentes	Write	incident-record*		
			response-plan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIncidentRecord	Otorga permiso para eliminar un registro de incidentes	Write	incident-record*		
DeleteReplicationSet	Otorga permiso para eliminar un conjunto de replicaciones	Write	replication-set*		
DeleteResourcePolicy	Otorga permiso para eliminar la política de recursos de un plan de respuesta	Permissions management	response-plan*		
DeleteResponsePlan	Otorga permiso para eliminar un plan de respuesta	Write	response-plan*		
DeleteTimelineEvent	Otorga permiso para eliminar un evento de línea de tiempo	Write	incident-record*		
GetIncidentRecord	Otorga permiso para ver el contenido de un registro de incidentes	Read	incident-record*		
			response-plan*		
GetReplicationSet	Otorga permiso para ver el conjunto de replicaciones	Read	replication-set*		
GetResourcePolicies	Otorga permiso para ver las políticas de recursos de un plan de respuesta	Read	response-plan*		
GetResponsePlan	Otorga permisos para ver el contenido de un plan de respuesta especificado	Read	response-plan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTimelineEvent	Otorga permiso para ver un evento de línea de tiempo	Lectura	incident-record*		
			response-plan*		
ListIncidentFindings	Concede permiso para enumerar resultados para un registro de incidentes	Enumeración	incident-record*		
			response-plan*		
ListIncidentRecords	Otorga permiso para enumerar el contenido de todos los registros de incidentes	Enumeración			
ListRelatedItems	Concede permiso para enumerar elementos relacionados de un registro de incidentes	Enumeración	incident-record*		
			response-plan*		
ListReplicationSets	Otorga permiso para mostrar todos los conjuntos de reproducción	List			
ListResponsePlans	Otorga permiso para enumerar todos los planes de respuesta	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para ver una lista de etiquetas de recurso para un recurso especificado	Read	incident-record		
			replication-set		
			response-plan		
ListTimelineEvents	Otorga permiso con el fin de enumerar todos los eventos de línea de tiempo para un registro de incidentes	List	incident-record*		
			response-plan*		
PutResourcePolicy	Otorga permiso para colocar la política de recursos en un plan de respuesta	Permissions management	response-plan*		
StartIncident	Otorga permiso para iniciar un nuevo incidente mediante un plan de respuesta	Write	response-plan*		
TagResource	Concede permiso para agregar etiquetas a un plan de respuesta	Etiquetado	incident-record		
			replication-set		
			response-plan		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para quitar etiquetas de un plan de respuesta	Etiquetado	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys	
UpdateDeletionProtection	Otorga permiso para actualizar la protección de eliminación de conjuntos de reproducción	Write	replication-set*		
UpdateIncidentRecord	Otorga permiso para actualizar el contenido de un registro de incidentes	Write	incident-record*		
			response-plan*		
UpdateRelatedItems	Otorga permiso para actualizar elementos relacionados de un registro de incidentes	Write	incident-record*		
			response-plan*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateReplicationSet	Otorga permiso para actualizar un conjunto de replicaciones	Write	replication-set*		
UpdateResponsePlan	Otorga permiso para actualizar el contenido de un plan de respuesta	Write	response-plan*		iam:PassRole ssm-incidents:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTimelineEvent	Otorga permiso para actualizar un evento de línea de tiempo	Write	incident-record*		
			response-plan*		

Tipos de recursos definidos por AWS Systems Manager Incident Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
response-plan	arn:${Partition}:ssm-incidents::${Account}:response-plan/${ResponsePlan}	aws:ResourceTag/${TagKey}
incident-record	arn:${Partition}:ssm-incidents::${Account}:incident-record/${ResponsePlan}/${IncidentRecord}	aws:ResourceTag/${TagKey}
replication-set	arn:${Partition}:ssm-incidents::${Account}:replication-set/${ReplicationSet}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Systems Manager Incident Manager Contacts

AWS Systems Manager Incident Manager Contacts (prefijo de servicio:`ssm-contacts`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Systems Manager Incident Manager Contacts
- Tipos de recursos definidos por AWS Systems Manager Incident Manager Contacts
- Claves de condición para AWS Systems Manager Incident Manager Contacts

Acciones definidas por AWS Systems Manager Incident Manager Contacts

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptPage	Concede permiso para aceptar una página	Write	page*		
ActivateContactChannel	Concede permiso para activar el canal de contacto de un contacto	Write	contactchannel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateContact [solo permiso]	Concede permiso para usar un contacto en un plan de escalado	Permissions management	contact*		
CreateContact	Concede permiso para crear un contacto	Write	contact*		ssm-contacts:AssociateContact
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContactChannel	Concede permiso para crear un canal de contacto para un contacto	Escritura	contact*		
CreateRotation	Concede permiso para crear una rotación en un horario de guardia	Escritura	rotation*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRotationOverride	Concede permiso para crear una anulación de una rotación en un horario de guardia	Escritura	rotation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeactivateContactChannel	Concede permiso para desactivar el canal de contacto de un contacto	Write	contactchannel*		
DeleteContact	Concede permiso para eliminar un contacto	Write	contact*		
DeleteContactChannel	Concede permiso para eliminar el canal de contacto de un contacto	Escritura	contactchannel*		
DeleteRotation	Concede permiso para eliminar una rotación	Escritura	rotation*		
DeleteRotationOverride	Concede permiso para eliminar la anulación de rotación de una rotación	Escritura	rotation*		
DescribeEngagement	Concede permiso para describir un compromiso	Read	engagement*		
DescribePage	Concede permiso para describir una página	Read	page*		
GetContact	Concede permiso para obtener un contacto	Read	contact*		
GetContactChannel	Concede permiso para obtener el canal de contacto de un contacto	Lectura	contactchannel*		
GetContactPolicy	Concede permiso para obtener la política de recursos de un contacto	Lectura	contact*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRotation	Concede permiso para recuperar información acerca de un horario de guardia	Lectura	rotation*		
GetRotationOverride	Concede permiso para recuperar información acerca de una anulación en un horario de guardia	Lectura	rotation*		
ListContactChannels	Concede permiso para enumerar todos los canales de contacto de un contacto	List	contact*		
ListContacts	Concede permiso para enumerar todos los contactos	List			
ListEngagements	Concede permiso para enumerar todas las interacciones	List			
ListPageReceipts	Concede permiso para enumerar todos los recibos de una página	Enumeración	page*		
ListPageResolutions	Otorga permiso para enumerar la ruta de resolución de una interacción	Enumeración	page*		
ListPagesByContact	Concede permiso para enumerar todas las páginas enviadas a un contacto	List	contact*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPagesByEngagement	Concede permiso para enumerar todas las páginas creadas en una interacción	Enumeración	engagement*		
ListPreviewRotationShifts	Concede permiso para recuperar una lista de turnos en función de los parámetros de configuración de rotación	Enumeración			
ListRotationOverrides	Concede permiso para recuperar una lista de anulaciones especificadas para una rotación de guardia	Enumeración	rotation*		
ListRotationShifts	Concede permiso para recuperar una lista de turnos de rotación en un horario de guardia	Enumeración	rotation*		
ListRotations	Concede permiso para recuperar una lista de rotaciones de guardia	Enumeración			
ListTagsForResource	Concede permiso para ver una lista de etiquetas de recurso para un recurso especificado	Lectura	contact rotation		
PutContactPolicy	Concede permiso para agregar una política de recursos a un contacto	Write	contact*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
SendActivationCode	Concede permiso para enviar el código de activación del canal de contacto de un contacto	Write	contactchannel*		
StartEngagement	Concede permiso para iniciar una interacción	Write	contact*		
StopEngagement	Concede permiso para detener una interacción	Escritura	engagement*		
TagResource	Otorga permiso para agregar etiquetas al recurso especificado	Etiquetado	contact		
			rotation		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas del recurso especificado	Etiquetado	contact		
			rotation		
				aws:TagKeys	
UpdateContact	Concede permiso para actualizar un contacto	Write	contact*		ssm-contacts:AssociateContact

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateContactChannel	Concede permiso para actualizar el canal de contacto de un contacto	Escritura	contactchannel*		
UpdateRotation	Concede permiso para actualizar la información especificada para una rotación de guardia	Escritura	rotation*		

Tipos de recursos definidos por AWS Systems Manager Incident Manager Contacts

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
contact	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contact/${ContactAlias}`	aws:ResourceTag/${TagKey}
contactchannel	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contactchannel/${ContactAlias}/${ContactChannelId}`	
engagement	`arn:${Partition}:ssm-contacts:${Region}:${Account}:engagement/${ContactAlias}/${EngagementId}`	

Tipos de recurso	ARN	Claves de condición
page	`arn:${Partition}:ssm-contacts:${Region}:${Account}:page/${ContactAlias}/${PageId}`	
rotation	`arn:${Partition}:ssm-contacts:${Region}:${Account}:rotation/${RotationId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Systems Manager Incident Manager Contacts

AWS Systems Manager Incident Manager Contacts define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para la Configuración Rápida de AWS Systems Manager

AWS La configuración rápida de Systems Manager (prefijo de servicio:`ssm-quicksetup`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la Configuración Rápida de AWS Systems Manager
- Tipos de recursos definidos por Configuración Rápida de AWS Systems Manager
- Claves de condición para la Configuración Rápida de AWS Systems Manager

Acciones definidas por la Configuración Rápida de AWS Systems Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye

un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateConfigurationManager	Concede permiso para crear un recurso de administrador de configuración de Configuración Rápida	Escritura	configuration-manager*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
DeleteConfigurationManager	Concede permiso para eliminar un administrador de configuración	Escritura	configuration-manager*		
GetConfiguration	Otorga permiso para obtener la configuración de Quick Setup	Lectura	configuration-manager		
GetConfigurationManager	Concede permiso para obtener un administrador de configuración	Lectura	configuration-manager*		
GetServiceSettings	Otorga permiso para configurar los ajustes de Quick Setup en la solicitud Cuenta de AWS y Región de AWS	Lectura			
ListConfigurationManagers	Concede permiso para enumerar los administradores de configuración de Configuración Rápida	Enumeración			
ListConfigurations	Otorga permiso para enumerar las configuraciones de Quick Setup	Enumeración	configuration-manager		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListQuickSetupTypes	Concede permiso para enumerar los tipos de Configuración Rápida disponibles	Lectura			
ListTagsForResource	Concede permiso para enumerar las etiquetas asignadas al recurso	Lectura	configuration-manager*		
TagResource	Otorga permiso para asignar pares de metadatos clave-valor a los recursos AWS	Etiquetado	configuration-manager*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas del recurso especificado	Etiquetado	configuration-manager*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateConfigurationDefinition	Concede permiso para actualizar una definición de configuración de Configuración Rápida	Escritura	configuration-manager*		
UpdateConfigurationManager	Concede permiso para actualizar un administrador de configuración de Configuración Rápida	Escritura	configuration-manager*		
UpdateServiceSettings	Concede permiso para actualizar los ajustes configurados para Configuración Rápida	Escritura			

Tipos de recursos definidos por Configuración Rápida de AWS Systems Manager

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
configuration-manager	`arn:${Partition}:ssm-quicksetup:${Region}:${Account}:configuration-manager/${ConfigurationManagerId}`	aws:ResourceTag/${TagKey}

Claves de condición para la Configuración Rápida de AWS Systems Manager

AWS La configuración rápida de Systems Manager define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Actions, resources, and condition keys for Tag Editor

El Editor de etiquetas (prefijo del servicio: `resource-explorer`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Tag Editor
- Tipos de recursos definidos por Tag Editor
- Claves de condición para Tag Editor

Acciones definidas por Tag Editor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourceTypes [solo permiso]	Concede permiso para recuperar los tipos de recursos admitidos actualmente en Tag Editor	List			
ListResources [solo permiso]	Otorga permiso para recuperar los identificadores de los recursos del Cuenta de AWS	Enumeración			
ListTags [solo permiso]	Concede permiso para recuperar las etiquetas asociadas a los identificadores de recursos especificados.	Read			tag:GetResources

Tipos de recursos definidos por Tag Editor

El Editor de etiquetas no admite especificar un ARN de recurso en el elemento `Resource` de una instrucción de política de IAM. Para permitir el acceso al Editor de etiquetas, especifique `"Resource": "*"` en la política.

Claves de condición para Tag Editor

Tag Editor no tiene claves de contexto específicas para servicios que puedan utilizarse en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para la configuración fiscal de AWS

AWS Tax Settings (prefijo de servicio:`tax`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por la configuración fiscal de AWS
- Tipos de recurso definidos por la configuración fiscal de AWS
- Claves de condición para la configuración fiscal de AWS

Acciones definidas por la configuración fiscal de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchDeleteTaxRegistration	Concede permiso para eliminar por lotes los datos de registros fiscales	Escritura			
BatchPutTaxRegistration	Concede permiso para actualizar por lotes los registros fiscales	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSupplementalTaxRegistration	Otorga permiso para eliminar los datos suplementarios del registro fiscal	Escritura			
DeleteTaxRegistration	Concede permiso para eliminar los datos de registros fiscales	Escritura			
GetExemptions	Concede permiso para visualizar los datos de las exenciones fiscales	Lectura			
GetTaxInfoReportingDocument [solo permiso]	Otorga permiso para gravar documentos y formularios view/download	Lectura			
GetTaxInheritance	Concede permiso para ver el estado de la herencia fiscal	Lectura			
GetTaxInterview [solo permiso]	Otorga permiso para recuperar los datos de entrevistas sobre impuestos	Lectura			
GetTaxRegistration	Otorga permiso para ver los datos de registros fiscales	Lectura			
GetTaxRegistrationDocument	Concede permiso para descargar los documentos de registros fiscales	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSupplementalTaxRegistrations	Otorga permiso para ver los registros tributarios complementarios	Lectura			
ListTaxRegistrations	Concede permiso para ver los registros fiscales	Lectura			
PutSupplementalTaxRegistration	Otorga permiso para actualizar los datos de los registros tributarios complementarios	Escritura			
PutTaxInheritance	Concede permiso para establecer la herencia fiscal	Escritura			
PutTaxInterview [solo permiso]	Otorga permiso para actualizar los datos de entrevistas sobre impuestos	Escritura			
PutTaxRegistration	Otorga permiso para actualizar los datos de registros fiscales	Escritura			
UpdateExemptions	Concede permiso para actualizar los datos de las exenciones fiscales	Escritura			

Tipos de recurso definidos por la configuración fiscal de AWS

AWS Tax Settings no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a la configuración fiscal de AWS , especifique `"Resource": "*"` en la política.

Claves de condición para la configuración fiscal de AWS

La configuración fiscal no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para AWS Telco Network Builder

AWS Telco Network Builder (prefijo de servicio:`tnb`) proporciona los siguientes recursos, acciones y claves contextuales de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Telco Network Builder
- Tipos de recurso definidos por AWS Telco Network Builder
- Claves de condición de AWS Telco Network Builder

Acciones definidas por AWS Telco Network Builder

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelSolNetworkOperation	Otorga permiso para cancelar una operación de red	Escritura	network-operation*		
CreateSolFunctionPackage	Otorga permiso para crear un paquete de funciones	Escritura	function-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkInstance	Otorga permiso para crear una instancia de red	Escritura	network-instance*		
			network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkPackage	Otorga permiso para crear un paquete de redes	Escritura	network-package*		
				aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys	
DeleteSolFunctionPackage	Otorga permiso para eliminar un paquete de funciones	Escritura	function-package*		
DeleteSolNetworkInstance	Otorga permiso para eliminar una instancia de red	Escritura	network-instance*		
DeleteSolNetworkPackage	Otorga permiso para eliminar un paquete de redes	Escritura	network-package*		
GetSolFunctionInstance	Otorga permiso para obtener una instancia de función	Lectura	function-instance*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackage	Otorga permiso para obtener un paquete de funciones	Lectura	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageContent	Otorga permiso para obtener el contenido de un paquete de funciones	Lectura	function-package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageDescriptor	Otorga permiso para obtener un descriptor de paquete de funciones	Lectura	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkInstance	Otorga permiso para obtener una instancia de red	Lectura	network-instance*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkOperation	Otorga permiso para obtener una operación de red	Lectura	network-operation*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackage	Otorga permiso para obtener un paquete de redes	Lectura	network-package*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSolNetworkPackageContent	Otorga permiso para obtener el contenido de un paquete de redes	Lectura	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageDescriptor	Otorga permiso para obtener un descriptor de paquete de redes	Lectura	network-package*		
				aws:ResourceTag/${TagKey}	
InstantiateSolNetworkInstance	Otorga permiso para instanciar una instancia de red	Escritura	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListSolFunctionInstances	Otorga permiso para enumerar las instancias de función	Enumeración	function-instance*		
				aws:ResourceTag/${TagKey}	
ListSolFunctionPackages	Otorga permiso para enumerar paquetes de funciones	Enumeración	function-package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
ListSolNetworkInstances	Otorga permiso para enumerar instancias de redes	Enumeración	network-instance*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkOperations	Otorga permiso para enumerar operaciones de redes	Enumeración	network-operation*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkPackages	Otorga permiso para enumerar paquetes de redes	Enumeración	network-package*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permiso para devolver una lista de etiquetas de un recurso	Enumeración			
PutSolFunctionPackageContent	Otorga permiso para cargar el contenido del paquete de funciones	Escritura	function-package*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutSolNetworkPackageContent	Otorga permiso para cargar el contenido de paquetes de redes	Escritura	network-package*		
TagResource	Otorga permiso para agregar etiquetas al recurso especificado	Etiquetado	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateSolNetworkInstance	Otorga permiso para terminar instancias de red	Escritura	network-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas del recurso especificado	Etiquetado	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys	
UpdateSolFunctionPackage	Otorga permiso para actualizar un paquete de función	Escritura	function-package*		
UpdateSolNetworkInstance	Otorga permiso para actualizar una instancia de red	Escritura	function-instance*		
			network-instance*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSolNetworkPackage	Otorga permiso para actualizar un paquete de red	Escritura	network-package*		
ValidateSolFunctionPackageContent	Otorga permiso para validar el contenido del paquete de funciones	Escritura	function-package*		
ValidateSolNetworkPackageContent	Otorga permiso para validar el contenido del paquete de red	Escritura	network-package*		

Tipos de recurso definidos por AWS Telco Network Builder

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
function-package	`arn:${Partition}:tnb:${Region}:${Account}:function-package/${FunctionPackageId}`	aws:ResourceTag/${TagKey}
network-package	`arn:${Partition}:tnb:${Region}:${Account}:network-package/${NetworkPackageId}`	aws:ResourceTag/${TagKey}
network-instance	`arn:${Partition}:tnb:${Region}:${Account}:network-instance/${NetworkInstanceId}`	aws:ResourceTag/${TagKey}
function-instance	`arn:${Partition}:tnb:${Region}:${Account}:function-instance/${FunctionInstanceId}`	aws:ResourceTag/${TagKey}
network-operation	`arn:${Partition}:tnb:${Region}:${Account}:network-operation/${NetworkOperationId}`	aws:ResourceTag/${TagKey}

Claves de condición de AWS Telco Network Builder

AWS Telco Network Builder define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante la comprobación de la presencia de pares de clave-valor de etiquetas en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso mediante la comprobación de los pares de clave-valor de las etiquetas adjuntas al recurso	Cadena
aws:TagKeys	Filtra el acceso según la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para Amazon Textract

Amazon Textract (prefijo de servicio `textract`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Textract
- Tipos de recurso definidos por Amazon Textract
- Claves de condición de Amazon Textract

Acciones definidas por Amazon Textract

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza

una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AnalyzeDocument	Otorga permiso para detectar instancias de entidades de documentos del mundo real dentro de una imagen proporcionada como entrada	Lectura			s3:GetObject
AnalyzeExpense	Otorga permiso para detectar instancias de entidades de documentos del mundo real dentro de una imagen proporcionada como entrada	Lectura			s3:GetObject
AnalyzeID	Otorga permiso para detectar información relevante de los documentos de identidad proporcionados como entrada.	Lectura			s3:GetObject
CreateAdapter	Concede permiso para crear un adaptador de Amazon Textract	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdapterVersion	Concede permiso para crear una versión del adaptador de Amazon Textract	Escritura	adapter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAdapter	Concede permiso para eliminar un adaptador de Amazon Textract	Escritura	adapter*		
DeleteAdapterVersion	Concede permiso para eliminar una versión del adaptador de Amazon Textract	Escritura	adapterversion*		
DetectDocumentText	Otorga permiso para detectar texto en imágenes de documentos	Lectura			s3:GetObject
GetAdapter	Concede permiso para obtener un adaptador de Amazon Textract	Lectura	adapter*		
GetAdapterVersion	Concede permiso para obtener una versión del adaptador de Amazon Textract	Lectura	adapterversion*		
GetDocumentAnalysis	Otorga permiso para devolver información sobre un trabajo de análisis de documento	Lectura			
GetDocumentTextDetection	Otorga permiso para devolver información sobre un trabajo de detección de documento de texto	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetExpenseAnalysis	Otorga permiso para devolver información acerca de un trabajo de análisis de gastos.	Lectura			
GetLendingAnalysis	Otorga permiso para recuperar información de nivel de página relativa a un trabajo de análisis de préstamos	Lectura			
GetLendingAnalysisSummary	Otorga permiso para recuperar información resumida relativa a un trabajo de análisis de préstamos	Lectura			
ListAdapterVersions	Concede permiso para enumerar las versiones del adaptador de Amazon Textract	Lectura			
ListAdapters	Concede permiso para enumerar los adaptadores de Amazon Textract	Lectura			
ListTagsForResource	Otorga permiso para devolver una lista de etiquetas asociadas a un recurso.	Lectura	adapter		
			adapterversion		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartDocumentAnalysis	Otorga permiso para comenzar un trabajo asíncrono para detectar instancias de entidades de documentos del mundo real dentro de una imagen o PDF proporcionado como entrada	Escritura			s3:GetObject
StartDocumentTextDetection	Otorga permiso para comenzar un trabajo asíncrono para detectar texto en PDF o imágenes de documentos	Escritura			s3:GetObject
StartExpenseAnalysis	Otorga permiso para comenzar un trabajo asíncrono para detectar instancias de facturas o recibos dentro de una imagen o PDF proporcionado como entrada.	Escritura			s3:GetObject
StartLendingAnalysis	Otorga permiso para iniciar un trabajo asíncrono para la detección de entidades en un documento de préstamo, toma una imagen o PDF proporcionado como entrada	Escritura			s3:GetObject
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso.	Etiquetado	adapter adapterversion		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	adapter		
			adapterversion		
				aws:TagKeys	
UpdateAdapter	Concede permiso para actualizar el adaptador de Amazon Textract	Escritura	adapter*		

Tipos de recurso definidos por Amazon Textract

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
adapter	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}`	aws:ResourceTag/${TagKey}
adapterversion	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}/versions/${AdapterVersion}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Textract

Amazon Textract define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Timestream

Amazon Timestream (prefijo de servicio: `timestream`) proporciona las claves de contexto de condición, acciones y recursos específicas de servicios siguientes para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Timestream
- Tipos de recurso definidos por Amazon Timestream
- Claves de condición de Amazon Timestream

Acciones definidas por Amazon Timestream

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelQuery	Otorga permiso para cancelar consultas en su cuenta	Escritura			timestream:DescribeEndpoints
CreateBatchLoadTask	Concede permiso para crear una tarea de carga por lotes en su cuenta	Escritura	table*		timestream:DescribeEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					timestream:WriteRecords
CreateDatabase	Otorga permisos para crear una base de datos en su cuenta.	Escritura	database*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledQuery	Otorga permiso para crear una consulta programada en su cuenta.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole timestream:DescribeEndpoints
CreateTable	Otorga permiso para crear una tabla en su cuenta.	Escritura	table*		timestream:DescribeEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatabase	Otorga permiso para eliminar una base de datos en su cuenta.	Escritura	database*		timestream:DescribeEndpoints
DeleteScheduledQuery	Otorga permiso para eliminar una consulta programada de su cuenta	Escritura	scheduled-query*		timestream:DescribeEndpoints
DeleteTable	Otorga permiso para eliminar una tabla en su cuenta.	Escritura	table*		timestream:DescribeEndpoints
DescribeAccountSettings	Concede permiso para describir la configuración de la cuenta	Lectura			timestream:DescribeEndpoints
DescribeBatchLoadTask	Concede permiso para describir una tarea de carga por lotes de su cuenta	Lectura			timestream:DescribeEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDatabase	Otorga permiso para describir una base de datos en su cuenta.	Lectura	database*		timestream:DescribeEndpoints
DescribeEndpoints	Otorga permiso para describir los puntos de conexión de la secuencia temporal.	Enumeración			
DescribeScheduledQuery	Otorga permiso para describir una consulta programada en su cuenta	Lectura	scheduled-query*		timestream:DescribeEndpoints
DescribeTable	Otorga permiso para describir una tabla en su cuenta.	Lectura	table*		timestream:DescribeEndpoints
ExecuteScheduledQuery	Otorga permiso para ejecutar una consulta programada en su cuenta.	Escritura	scheduled-query*		timestream:DescribeEndpoints
GetAwsBackupStatus	Otorga permiso para obtener el estado de una copia de seguridad de una tabla de Timestream	Lectura			timestream:DescribeEndpoints
GetAwsRestoreStatus	Otorga permiso para obtener el estado de una restauración de una tabla de Timestream	Lectura			timestream:DescribeEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListBatchLoadTasks	Concede permiso para enumerar tareas de carga por lotes de su cuenta	Enumeración			timestream:DescribeEndpoints
ListDatabases	Otorga permiso para enumerar las bases de datos en su cuenta.	Enumeración			timestream:DescribeEndpoints
ListMeasures	Otorga permiso. para enumerar las medidas de una tabla en su cuenta	Enumeración	table*		timestream:DescribeEndpoints
ListScheduledQueries	Otorga permiso para enumerar las programaciones en su cuenta.	Enumeración			timestream:DescribeEndpoints
ListTables	Otorga permiso para enumerar las aplicaciones en su cuenta	Enumeración	database*		timestream:DescribeEndpoints
ListTagsForResource	Otorga permiso para enumerar etiquetas de un recurso en su cuenta.	Lectura	database*		timestream:DescribeEndpoints
			scheduled-query*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			table*		
PrepareQuery	Otorga permiso para emitir consultas de preparación	Lectura	table*		timestream:DescribeEndpoints timestream:Select
ResumeBatchLoadTask	Concede permiso para reanudar una tarea de carga por lotes de su cuenta	Escritura			timestream:DescribeEndpoints timestream:WriteRecords
Select	Otorga permiso para emitir consultas "select from table"	Lectura	table*		timestream:DescribeEndpoints
SelectValues	Otorga permiso para emitir consultas "select 1".	Lectura			timestream:DescribeEndpoints
StartAwsBackupJob	Otorga permiso para iniciar un trabajo de copia de seguridad de una tabla de Timestream	Escritura	table*		timestream:DescribeEndpoints

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartAwsRestoreJob	Otorga permiso para iniciar un trabajo de restauración de una copia de seguridad de una tabla de Timestream	Escritura	table*		timestream:DescribeEndpoints
TagResource	Otorga permiso para agregar etiquetas a un recurso	Etiquetado	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Unload	Concede permiso para emitir consultas de descarga	Escritura	table*		s3:AbortMultipartUpload s3:GetObject s3:PutObject timestream:DescribeEndpoints timestream:Select
UntagResource	Otorga permiso para eliminar una etiqueta de un recurso.	Etiquetado	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAccountSettings	Concede permiso para actualizar la configuración de la cuenta	Escritura			timestream:DescribeEndpoints
UpdateDatabase	Otorga permiso para actualizar una base de datos en su cuenta.	Escritura	database*		timestream:DescribeEndpoints
UpdateScheduledQuery	Otorga permiso para actualizar una consulta programada en su cuenta.	Escritura	scheduled-query*		timestream:DescribeEndpoints
UpdateTable	Otorga permiso para actualizar una tabla en su cuenta.	Escritura	table*		timestream:DescribeEndpoints
WriteRecords	Otorga permiso para capturar datos en una tabla de su cuenta.	Escritura	table*		timestream:DescribeEndpoints

Tipos de recurso definidos por Amazon Timestream

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
database	`arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}/table/${TableName}`	aws:ResourceTag/${TagKey}
scheduled-query	`arn:${Partition}:timestream:${Region}:${Account}:scheduled-query/${ScheduledQueryName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Timestream

Amazon Timestream define las siguientes claves de condiciones que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Amazon Timestream InfluxDB

Amazon Timestream InfluxDB (prefijo del servicio: `timestream-influxdb`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Timestream InfluxDB
- Tipos de recursos definidos por Amazon Timestream InfluxDB
- Claves de condición para Amazon Timestream InfluxDB

Acciones definidas por Amazon Timestream InfluxDB

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateDbCluster	Otorga permiso para crear un nuevo clúster de Timestream InfluxDB	Escritura	db-parameter-group		timestream-influxdb:CreateDbInstance
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbInstance	Concede permiso para crear una nueva instancia de Timestream InfluxDB	Escritura	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	Concede permiso para crear un nuevo grupo de parámetros de Timestream InfluxDB	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbCluster	Otorga permiso para eliminar un clúster InfluxDB de Timestream	Escritura	db-cluster*		timestream-influxdb:DeleteD

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					bInstance
DeleteDbInstance	Concede permiso para eliminar una instancia de Timestream InfluxDB	Escritura	db-instance*		
GetDbCluster	Otorga permiso para obtener información sobre un clúster InfluxDB de Timestream	Lectura	db-cluster*		
GetDbInstance	Concede permiso para obtener información sobre una instancia de Timestream InfluxDB	Lectura	db-instance*		
GetDbParameterGroup	Concede permiso para obtener información sobre un grupo de parámetros de Timestream InfluxDB	Lectura	db-parameter-group*		
ListDbClusters	Otorga permiso para incluir información sobre todos los clústeres de Timestream InfluxDB de la cuenta	Enumeración			
ListDbInstances	Concede permiso para enumerar información sobre todas las instancias de Timestream InfluxDB en la cuenta	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListDbInstancesForCluster	Otorga permiso para incluir información sobre todas las instancias de Timestream InfluxDB que pertenecen a un clúster	Lectura	db-cluster*		
ListDbParameterGroups	Concede permiso para enumerar información sobre todos los grupos de parámetros de Timestream InfluxDB	Enumeración			
ListTagsForResource	Concede permiso para enumerar etiquetas para un recurso de Timestream InfluxDB	Lectura	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para etiquetar un recurso de Timestream InfluxDB	Etiquetado	db-cluster		
			db-instance		
			db-parameter-group		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para quitar etiquetas de un recurso de Timestream InfluxDB	Etiquetado	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbCluster	Otorga permiso para actualizar un clúster de Timestream InfluxDB	Escritura	db-cluster*		timestream-influxdb:UpdateDbInstance

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			db-parameter-group		
UpdateDbInstance	Concede permiso para actualizar una instancia de Timestream InfluxDB	Escritura	db-instance*		
			db-parameter-group		

Tipos de recursos definidos por Amazon Timestream InfluxDB

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
db-cluster	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-cluster/${DbClusterId}`	aws:ResourceTag/${TagKey}
db-instance	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-instance/${DbInstanceIdentifier}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
db-parameter-group	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Timestream InfluxDB

Amazon Timestream InfluxDB define las siguientes claves de condición que se pueden usar en el elemento `Condition` de una instrucción de política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Tiros

AWS Tiros (prefijo de servicio:`tiros`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Tiros
- Tipos de recursos definidos por AWS Tiros
- Claves de condición para AWS Tiros

Acciones definidas por AWS Tiros

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateQuery [solo permiso]	Concede permiso para crear una consulta de accesibilidad de VPC	Write			
ExtendQuery [solo permiso]	Concede permiso para extender una consulta de accesibilidad de la VPC para incluir la cuenta de la entidad principal solicitante	Escritura			
GetQueryAnswer [solo permiso]	Concede permiso para obtener respuestas de consulta de accesibilidad de VPC	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetQueryExplanation [solo permiso]	Concede permiso para obtener explicaciones de consulta de accesibilidad de VPC	Lectura			
GetQueryExtensionAccounts [solo permiso]	Concede permiso para enumerar las cuentas que podrían ser útiles en una consulta nueva	Lectura			

Tipos de recursos definidos por AWS Tiros

AWS Tiros no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS Tiros, especifique `"Resource": "*"` en su política.

Claves de condición para AWS Tiros

Tiros no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de la política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Transcribe

Amazon Transcribe (prefijo de servicio: `transcribe`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para usarlas en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Transcribe
- Tipos de recurso definidos por Amazon Transcribe
- Claves de condición de Amazon Transcribe

Acciones definidas por Amazon Transcribe

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateCallAnalyticsCategory	Otorga permiso para crear una categoría de análisis. Amazon Transcribe aplica las condiciones especificadas por las categorías de análisis a sus trabajos de análisis de llamadas	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLanguageModel	Otorga permiso para crear un nuevo modelo de idioma personalizado	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateMedicalVocabulary	Otorga permiso para crear un nuevo vocabulario personalizado que se puede utilizar para cambiar el modo en que Amazon Transcribe Medical	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	administra la transcripción de un archivo de audio				
CreateVocabulary	Otorga permiso para crear un nuevo vocabulario personalizado que se puede utilizar para cambiar la manera en la que Amazon Transcribe administra la transcripción de un archivo de audio	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabularyFilter	Otorga permiso para crear un nuevo filtro de vocabulario que puede utilizar para filtrar palabras de la transcripción de un archivo de audio generado por Amazon Transcribe	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	Otorga permiso para eliminar una categoría de análisis de llamadas mediante su nombre de Amazon Transcribe	Write	callanalyticscategory*		
DeleteCallAnalyticsJob	Otorga permiso para eliminar un trabajo de análisis de llamadas enviado previamente junto con cualquier otro resultado generado, como de transcripción, modelos, etc.	Write	callanalyticsjob*		
DeleteLanguageModel	Otorga permiso para eliminar un modelo de idioma personalizado creado anteriormente	Escritura	languagemodel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMedicalScribeJob	Otorga permiso para eliminar un trabajo de Medical Scribe previamente enviado	Escritura	medicalscribejob*		
DeleteMedicalTranscriptionJob	Otorga permiso para eliminar un trabajo de transcripción médica previamente enviado	Write	medicaltranscriptionjob*		
DeleteMedicalVocabulary	Otorga permiso para eliminar un vocabulario médico de Amazon Transcribe	Write	medicalvocabulary*		
DeleteTranscriptionJob	Otorga permiso para eliminar un trabajo de transcripción enviado previamente junto con cualquier otro resultado generado, como de transcripción, modelos, etc.	Write	transcriptionjob*		
DeleteVocabulary	Otorga permiso para eliminar un vocabulario de Amazon Transcribe	Write	vocabulary*		
DeleteVocabularyFilter	Otorga permiso para eliminar un filtro de vocabulario de Amazon Transcribe	Write	vocabularyfilter*		
DescribeLanguageModel	Otorga permiso para devolver información sobre un modelo de idioma personalizado	Read	languagemodel*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetCallAnalyticsCategory	Otorga permiso para recuperar información sobre una categoría de análisis de llamadas	Read	callanalyticscategory*		
GetCallAnalyticsJob	Otorga permiso para devolver información sobre un trabajo de análisis de llamadas	Lectura	callanalyticsjob*		
GetMedicalScribeJob	Otorga permiso para devolver información sobre un trabajo de Medical Scribe	Lectura	medicalscribejob*		
GetMedicalScribeStream	Otorga permiso para obtener información sobre la sesión de AWS HealthScribe streaming especificada	Lectura			
GetMedicalTranscriptionJob	Otorga permiso para devolver información sobre un trabajo de transcripción médica	Read	medicaltranscriptionjob*		
GetMedicalVocabulary	Otorga permiso para obtener información sobre un vocabulario médico	Read	medicalvocabulary*		
GetTranscriptionJob	Otorga permiso para devolver información sobre un trabajo de transcripción	Read	transcriptionjob*		
GetVocabulary	Otorga permiso para obtener información sobre un vocabulario	Read	vocabulary*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetVocabularyFilter	Otorga permiso para obtener información sobre un filtro de vocabulario	Read	vocabularyfilter*		
ListCallAnalyticsCategories	Otorga permiso para enumerar las categorías de análisis de llamadas que se han creado	List			
ListCallAnalyticsJobs	Otorga permiso para enumerar trabajos de análisis con el estado especificado	List			
ListLanguageModels	Otorga permiso para enumerar los modelos de idioma personalizados	Enumeración			
ListMedicalScribeJobs	Otorga permiso para enumerar trabajos de Medical Scribe con el estado especificado	Enumeración			
ListMedicalTranscriptionJobs	Otorga permiso para enumerar trabajos de transcripción médica con el estado especificado	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMedicalVocabularies	Otorga permiso para devolver una lista de vocabularios médicos que coinciden con los criterios especificados. Si no se especifican criterios, devuelve toda la lista de vocabularios	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
ListTranscriptionJobs	Otorga permiso para enumerar trabajos de transcripción con el estado especificado	List			
ListVocabularies	Otorga permiso para devolver una lista de vocabularios que coincidan con los criterios especificados. Si no se especifican criterios, devuelve toda la lista de vocabularios	List			
ListVocabularyFilters	Otorga permiso para devolver una lista de filtros de vocabulario que coincidan con los criterios especificados. Si no se especifican criterios, devuelve como máximo 5 filtros de vocabulario	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartCallAnalyticsJob	Otorga permiso para iniciar un trabajo de análisis asíncrono que no solo transcriba la grabación de audio de una persona que llama y un agente, sino que también devuelva información adicional	Escritura		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartCallAnalyticsStreamTranscription	Otorga permiso para iniciar un protocolo en el que el audio se transmite a Transcribe Call Analytics y los resultados de la transcripción se transmiten a su aplicación	Escritura			
StartCallAnalyticsStreamTranscriptionWebSocket	Otorga permiso para iniciar una WebSocket en la que el audio se transmite a Transcribe Call Analytics y los resultados de la transcripción se transmiten a su aplicación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartMedicalScribeJob	Otorga permiso para iniciar un trabajo asincrónico para transcribir las conversaciones entre el paciente y el médico y genera notas clínicas	Escritura		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	Otorga permiso para iniciar una HTTP2 transmisión bidireccional en la que se transmite el audio AWS HealthScribe y los resultados de la transcripción se transmiten a su aplicación	Escritura			
StartMedicalStreamTranscription	Otorga permiso para iniciar un protocolo donde el audio se transmite a Transcribe Medical, y los resultados de la transcripción se transmiten a la aplicación	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartMedicalStreamTranscriptionWebSocket	Otorga permiso para iniciar una WebSocket en la que el audio se transmite a Transcribe Medical y los resultados de la transcripción se transmiten a su aplicación	Escritura			
StartMedicalTranscriptionJob	Otorga permiso para iniciar un trabajo asincrónico para transcribir el habla médica en texto	Escritura		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	Otorga permiso para iniciar una HTTP2 transmisión bidireccional para transcribir voz a texto en tiempo real	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartStreamTranscriptionWebSocket	Otorga permiso para iniciar una transmisión websocket para transcribir la voz a texto en tiempo real	Write			
StartTranscriptionJob	Otorga permiso para iniciar un trabajo asíncrono para transcribir la voz a texto	Escritura		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para desetiquetar un recurso con la clave dada	Etiquetado		aws:TagKeys	
UpdateCallAnalyticsCategory	Otorga permiso para actualizar la categoría de análisis de llamadas con nuevos valores La UpdateCallAnalyticsCategory operación sobrescribe toda la información existente con los valores que proporcione en la solicitud	Escritura	callanalyticscategory*		
UpdateMedicalVocabulary	Otorga permiso para actualizar un vocabulario médico existente con nuevos valores. La UpdateMedicalVocabulary operación sobrescribe toda la información existente con los valores que proporcione en la solicitud	Escritura	medicalvocabulary*		s3:GetObject
UpdateVocabulary	Otorga permiso para actualizar un vocabulario existente con nuevos valores. La UpdateVocabulary operación sobrescribe toda la información existente con los valores que proporcione en la solicitud	Escritura	vocabulary*		s3:GetObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateVocabularyFilter	Otorga permiso para actualizar un filtro de vocabulario existente con nuevos valores. La UpdateVocabularyFilter operación sobrescribe toda la información existente con los valores que proporcione en la solicitud	Escritura	vocabularyfilter*		s3:GetObject

Tipos de recurso definidos por Amazon Transcribe

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
transcriptionjob	`arn:${Partition}:transcribe:${Region}:${Account}:transcription-job/${JobName}`	aws:ResourceTag/${TagKey}
vocabulary	`arn:${Partition}:transcribe:${Region}:${Account}:vocabulary/${VocabularyName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
vocabularyfilter	arn:${Partition}:transcribe:${Region}:${Account}:vocabulary-filter/${VocabularyFilterName}	aws:ResourceTag/${TagKey}
languagemodel	arn:${Partition}:transcribe:${Region}:${Account}:language-model/${ModelName}	aws:ResourceTag/${TagKey}
medicaltranscriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:medical-transcription-job/${JobName}	aws:ResourceTag/${TagKey}
medicalvocabulary	arn:${Partition}:transcribe:${Region}:${Account}:medical-vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}
callanalyticsjob	arn:${Partition}:transcribe:${Region}:${Account}:analytics/${JobName}	aws:ResourceTag/${TagKey}
callanalyticscategory	arn:${Partition}:transcribe:${Region}:${Account}:analytics-category/${CategoryName}	aws:ResourceTag/${TagKey}
medicalscribejob	arn:${Partition}:transcribe:${Region}:${Account}:medical-scribe-job/${JobName}	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Transcribe

Amazon Transcribe define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso requiriendo los valores de las etiquetas presentes en una solicitud de creación de recursos	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso requiriendo el valor de la etiqueta asociada al recurso	Cadena
aws:TagKeys	Filtra el acceso requiriendo la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
transcribe:OutputBucketName	Filtra el acceso en función del nombre del bucket de salida incluido en la solicitud	Cadena
transcribe:OutputEncryptionKMSKeyId	Filtra el acceso en función del ID de clave de KMS incluido en la solicitud	Cadena
transcribe:OutputKey	Filtra el acceso en función de la clave de salida incluida en la solicitud	Cadena
transcribe:OutputLocation	Filtra el acceso en función de la ubicación de salida incluida en la solicitud	Cadena

Claves de condición, acciones y recursos para AWS Transfer Family

AWS Transfer Family (prefijo de servicio:`transfer`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Transfer Family
- Tipos de recursos definidos por AWS Transfer Family
- Claves de condición para AWS Transfer Family

Acciones definidas por AWS Transfer Family

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAccess	Otorga permiso para agregar un acceso asociado a un servidor	Escritura	server*		iam:PassRole
CreateAgreement	Otorga permiso para agregar un acuerdo asociado a un servidor	Escritura	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnector	Concede permiso para crear un conector	Escritura		aws:TagKeys	iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey}	
CreateProfile	Otorga permiso para crear un perfil	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateServer	Otorga permiso para crear un servidor.	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateUser	Otorga permiso para agregar un usuario asociado a un servidor.	Escritura	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWebApp	Otorga permiso para crear una aplicación web	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateWorkflow	Concede permiso para crear un flujo de trabajo	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccess	Otorga permiso para eliminar el acceso	Escritura	server*		
DeleteAgreement	Otorga permiso para eliminar un acuerdo	Escritura	agreement*		
DeleteCertificate	Otorga permiso para eliminar un certificado	Escritura	certificate*		
DeleteConnector	Concede permiso para eliminar un conector	Escritura	connector*		
DeleteHostKey	Otorga permiso para eliminar una clave de host asociada a un servidor	Escritura	host-key*		
DeleteProfile	Otorga permiso para eliminar un perfil	Escritura	profile*		
DeleteServer	Otorga permiso para eliminar un servidor.	Write	server*		
DeleteSshPublicKey	Otorga permiso para eliminar una clave pública SSH de un usuario.	Write	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteUser	Otorga permiso para eliminar un usuario asociado a un servidor.	Escritura	user*		
DeleteWebApp	Otorga permiso para eliminar la aplicación web	Escritura	webapp*		
DeleteWebAppCustomization	Otorga permiso para eliminar la personalización de la aplicación web	Escritura	webapp*		
DeleteWorkflow	Concede permiso para eliminar un flujo de trabajo	Escritura	workflow*		
DescribeAccess	Otorga permiso para describir un acceso asociado a un servidor	Lectura	server*		
DescribeAgreement	Otorga permiso para describir un acuerdo asignado a un servidor	Lectura	agreement*		
DescribeCertificate	Otorga permiso para describir un certificado	Lectura	certificate*		
DescribeConnector	Otorga permiso para describir un conector	Lectura	connector*		
DescribeExecution	Otorga permiso para describir una ejecución asociada a un flujo de trabajo	Lectura	workflow*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeHostKey	Otorga permiso para describir una clave de host asociada a un servidor	Lectura	host-key*		
DescribeProfile	Otorga permiso para describir un perfil	Lectura	profile*		
DescribeSecurityPolicy	Otorga permiso para describir una política de seguridad.	Read			
DescribeServer	Otorga permiso para describir un servidor.	Read	server*		
DescribeUser	Otorga permiso para describir un usuario asociado a un servidor.	Lectura	user*		
DescribeWebApp	Otorga permiso para describir una aplicación web	Lectura	webapp*		
DescribeWebAppCustomization	Otorga permiso para describir la personalización de una aplicación web	Lectura	webapp*		
DescribeWorkflow	Otorga permiso para describir un flujo de trabajo	Lectura	workflow*		
ImportCertificate	Otorga permiso para agregar un certificado	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportHostKey	Otorga permiso para agregar una clave de host a un servidor	Escritura	server*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportSshPublicKey	Otorga permiso para agregar una clave pública SSH a un usuario.	Escritura	user*		
ListAccesses	Otorga permiso para enumerar accesos	Lectura	server*		
ListAgreements	Otorga permiso para enumerar acuerdos	Lectura	server*		
ListCertificates	Otorga permiso para enumerar certificados	Lectura			
ListConnectors	Otorga permiso para enumerar conectores	Lectura			
ListExecutions	Otorga permiso para enumerar ejecuciones asociadas a un flujo de trabajo	Lectura	workflow*		
ListFileTransferResults	Concede permiso para enumerar los estados de transferencia de archivos para conectores	Lectura	connector*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListHostKeys	Otorga permiso para enumerar las claves de host asociadas a un servidor	Lectura	server*		
ListProfiles	Otorga permiso para enumerar perfiles.	Lectura			
ListSecurityPolicies	Otorga permiso para mostrar una lista de políticas de seguridad.	List			
ListServers	Otorga permiso para mostrar una lista de servidores.	Enumeración			
ListTagsForResource	Otorga permiso para incluir etiquetas para un recurso AWS de Transfer Family	Lectura	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	Otorga permiso para mostrar una lista de los usuarios asociados a un servidor.	Enumeración	server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWebApps	Otorga permiso para enumerar aplicaciones web	Enumeración			
ListWorkflows	Otorga permiso para enumerar flujos de trabajo	Enumeración			
SendWorkflowStepState	Otorga permiso para enviar una devolución de llamada para pasos personalizados asíncronos	Escritura	workflow*		
StartDirectoryListing	Concede permiso para iniciar una operación de enumerar en un servidor remoto mediante un conector	Escritura	connector*		
StartFileTransfer	Otorga permiso para iniciar una transferencia de archivos de conector	Escritura	connector*		
StartRemoteDelete	Otorga permiso para iniciar una operación de eliminación de conectores en un servidor remoto	Escritura	connector*		
StartRemoteMove	Otorga permiso para iniciar una operación de traslado de un conector en un servidor remoto	Escritura	connector*		
StartServer	Otorga permiso para iniciar un servidor.	Write	server*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StopServer	Otorga permiso para detener un servidor.	Escritura	server*		
TagResource	Otorga permiso para etiquetar un recurso AWS de Transfer Family	Etiquetado	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	Otorga permiso para probar la conexión de un conector al servidor remoto	Escritura	connector*		
TestIdentityProvider	Otorga permiso para probar un proveedor de identidad personalizada de servidor.	Lectura	user*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para desetiquetar un recurso de AWS Transfer Family	Etiquetado	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		
				aws:TagKeys	
UpdateAccess	Otorga permiso para actualizar el acceso	Escritura			iam:PassRole
UpdateAgreement	Otorga permiso para actualizar un acuerdo	Escritura	agreement*		iam:PassRole
UpdateCertificate	Otorga permiso para actualizar un certificado	Escritura	certificate*		
UpdateConnector	Otorga permiso para actualizar un conector	Escritura	connector*		iam:PassRole
UpdateHostKey	Otorga permiso para actualizar una clave de host	Escritura	host-key*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateProfile	Otorga permiso para actualizar un perfil.	Escritura	profile*		
UpdateServer	Otorga permiso para actualizar la configuración de un servidor.	Write	server*		iam:PassRole
UpdateUser	Otorga permiso para actualizar la configuración de un usuario.	Escritura	user*		iam:PassRole
UpdateWebApp	Otorga permiso para actualizar la configuración de una aplicación web	Escritura	webapp*		iam:PassRole
UpdateWebAppCustomization	Otorga permiso para actualizar la configuración de la personalización de una aplicación web	Escritura	webapp*		iam:PassRole

Tipos de recursos definidos por AWS Transfer Family

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
user	arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}	aws:ResourceTag/${TagKey}
server	arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}	aws:ResourceTag/${TagKey}
certificate	arn:${Partition}:transfer:${Region}:${Account}:certificate/${CertificateId}	aws:ResourceTag/${TagKey}
connector	arn:${Partition}:transfer:${Region}:${Account}:connector/${ConnectorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:transfer:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
agreement	arn:${Partition}:transfer:${Region}:${Account}:agreement/${ServerId}/${AgreementId}	aws:ResourceTag/${TagKey}
host-key	arn:${Partition}:transfer:${Region}:${Account}:host-key/${ServerId}/${HostKeyId}	aws:ResourceTag/${TagKey}
webapp	arn:${Partition}:transfer:${Region}:${Account}:webapp/${WebAppId}	aws:ResourceTag/${TagKey}

Claves de condición para AWS Transfer Family

AWS Transfer Family define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las

condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de AWS Transform

AWS Transform (prefijo de servicio:`transform`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Transform AWS
- Tipos de recursos definidos por Transform AWS
- Claves de condición para AWS Transform

Acciones definidas por Transform AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateConnectorResource [solo permiso]	Otorga permiso para AssociateConnectorResource invocar en Transform AWS	Escritura			
CreateProfile [solo permiso]	Otorga permiso para CreateProfile invocar en Transform AWS	Escritura	profile*		
DeleteProfile [solo permiso]	Otorga permiso para DeleteProfile invocar en Transform AWS	Escritura	profile*		
GetConnector [solo permiso]	Otorga permiso para GetConnector invocar en Transform AWS	Lectura			
ListProfiles [solo permiso]	Otorga permiso para ListProfiles invocar en Transform AWS	Enumeración			
RejectConnector [solo permiso]	Otorga permiso para RejectConnector invocar en Transform AWS	Escritura			
UpdateProfile [solo permiso]	Otorga permiso para UpdateProfile invocar en Transform AWS	Escritura	profile*		

Tipos de recursos definidos por Transform AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
profile	`arn:${Partition}:transform:${Region}:${Account}:profile/${Identifier}`	

Claves de condición para AWS Transform

Transform no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Translate

Amazon Translate (prefijo de servicio: `translate`) proporciona las siguientes claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Translate

- Tipos de recurso definidos por Amazon Translate
- Claves de condición de Amazon Translate

Acciones definidas por Amazon Translate

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateParallelData	Concede permiso para crear datos paralelos.	Write	parallel-data		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteParallelData	Concede permiso para eliminar datos paralelos.	Write	parallel-data		
DeleteTerminology	Concede permiso para eliminar terminología	Write	terminology		
DescribeTextTranslationJob	Concede permiso para obtener las propiedades asociadas al trabajo de traducción por lotes asincrónico	Read			
GetParallelData	Concede permiso para obtener datos paralelos	Read	parallel-data		
GetTerminology	Concede permiso para recuperar terminología	Read	terminology		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ImportTerminology	Concede permiso para crear o actualizar una terminología, según si ya existe o no una con el nombre de terminología proporcionado	Escritura	terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListLanguages	Concede permiso para enumerar idiomas admitidos	Enumeración			
ListParallelData	Concede permiso para enumerar datos paralelos asociados a su cuenta	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	parallel-data		
			terminology		
ListTerminologies	Concede permiso para enumerar terminologías asociadas a su cuenta	List			
ListTextTranslationJobs	Concede permiso para enumerar los trabajos de traducción por lotes que ha enviado	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartTextTranslationJob	Concede permiso para iniciar un trabajo de traducción por lotes asincrónico. Los trabajos de traducción por lotes se pueden utilizar para traducir grandes volúmenes de texto de varios documentos a la vez	Write	parallel-data		
			terminology		
StopTextTranslationJob	Concede permiso para detener un trabajo de traducción por lotes asincrónico que está en curso	Escritura			
TagResource	Concede permiso para etiquetar un recurso con pares de valores de clave dados	Etiquetado	parallel-data		
			terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
TranslateDocument	Concede permiso para traducir un documento de un idioma de origen a un idioma de destino	Lectura	terminology		
TranslateText	Concede permiso para traducir texto de un idioma de origen a un idioma de destino	Lectura	parallel-data		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			terminology		
UntagResource	Concede permiso para desetiquetar un recurso con la clave dada	Etiquetado	parallel-data		
			terminology		
				aws:TagKeys	
UpdateParallelData	Concede permiso para actualizar datos paralelos existentes	Write	parallel-data		

Tipos de recurso definidos por Amazon Translate

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
terminology	`arn:${Partition}:translate:${Region}:${Account}:terminology/${ResourceName}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
parallel-data	`arn:${Partition}:translate:${Region}:${Account}:parallel-data/${ResourceName}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon Translate

Amazon Translate define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso requiriendo los valores de las etiquetas presentes en una solicitud de creación de recursos	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso requiriendo el valor de la etiqueta asociada al recurso	Cadena
aws:TagKeys	Filtra el acceso requiriendo la presencia de etiquetas obligatorias en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS Trusted Advisor

AWS Trusted Advisor (prefijo de servicio:`trustedadvisor`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Trusted Advisor
- Tipos de recursos definidos por AWS Trusted Advisor
- Claves de condición para AWS Trusted Advisor

Acciones definidas por AWS Trusted Advisor

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

> **Note**
>
> Los detalles de la descripción de la política de IAM Trusted Advisor solo se aplican a la consola de Trusted Advisor. Si desea gestionar el acceso programático a Trusted Advisor, utilice las operaciones de Trusted Advisor en la AWS Support API.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchUpdateRecommendationResourceExclusion	Concede permiso para actualizar uno o más estados de exclusión para una lista de recursos de recomendación	Escritura			
CreateEngagement	Concede permiso para crear una interacción	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEngagementAttachment	Concede permiso para crear un adjunto de interacción	Escritura			
CreateEngagementCommunication	Concede permiso para crear una comunicación de interacción	Escritura			
DeleteNotificationConfigurationForDelegatedAdmin	Concede permiso a la cuenta de administración de la organización para eliminar las preferencias de notificación por correo electrónico de una cuenta de administrador delegado de Trusted Advisor Priority	Escritura			
DescribeAccount [solo permiso]	Otorga permiso para ver el AWS Support plan y varias preferencias AWS de Trusted Advisor	Lectura			
DescribeAccountAccess [solo permiso]	Otorga permiso para ver si Cuenta de AWS ha activado o desactivado AWS Trusted Advisor	Lectura			
DescribeCheckItems	Concede permiso para ver los detalles de los elementos de comprobación	Lectura	checks*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeCheckRefreshStatuses	Otorga permiso para ver los estados de actualización de las comprobaciones de AWS Trusted Advisor	Lectura	checks*		
DescribeCheckStatusHistoryChanges [solo permiso]	Concede permiso para ver los resultados y estados modificados de las comprobaciones de los últimos 30 días	Lectura	checks*		
DescribeCheckSummaries	Otorga permiso para ver los resúmenes de cheques de AWS Trusted Advisor	Lectura	checks*		
DescribeChecks	Otorga permiso para ver los detalles de las comprobaciones AWS de Trusted Advisor	Lectura			
DescribeNotificationConfigurations	Concede permiso para obtener las preferencias de notificación por correo electrónico para Trusted Advisor Priority	Lectura			
DescribeNotificationPreferences [solo permiso]	Otorga permiso para ver las preferencias de notificación del Cuenta de AWS	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeOrganization [solo permiso]	Otorga permiso para ver si Cuenta de AWS cumple los requisitos para habilitar la función de visualización organizacional	Lectura			
DescribeOrganizationAccounts [solo permiso]	Otorga permiso para ver las AWS cuentas vinculadas que están en la organización	Lectura			
DescribeReports [solo permiso]	Concede permiso para ver los detalles de los informes de vista organizativa, como el nombre del informe, el tiempo de ejecución, la fecha de creación, el estado y el formato	Lectura			
DescribeRisk	Otorga permiso para ver los detalles de los riesgos en AWS Trusted Advisor Priority	Lectura			
DescribeRiskResources	Otorga permiso para ver los recursos afectados por un riesgo en AWS Trusted Advisor Priority	Lectura			
DescribeRisks	Otorga permiso para ver los riesgos en AWS Trusted Advisor Priority	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeServiceMetadata [solo permiso]	Otorga permiso para ver información sobre los informes de visualización de la organización, como las categorías de comprobación Regiones de AWS, los nombres de las comprobaciones y el estado de los recursos	Lectura			
DownloadRisk	Concede permiso para descargar un archivo que contiene detalles sobre el riesgo en AWS Trusted Advisor Priority	Lectura			
ExcludeCheckItems [solo permiso]	Otorga permiso para excluir las recomendaciones de las comprobaciones AWS de Trusted Advisor	Escritura	checks*		
GenerateReport [solo permiso]	Otorga permiso para crear un informe para los cheques de AWS Trusted Advisor en su organización	Escritura			
GetEngagement	Concede permiso para ver una interacción	Lectura			
GetEngagementAttachment	Concede permiso para ver un adjunto de interacción	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEngagementType	Concede permiso para ver un tipo de interacción específico	Lectura			
GetOrganizationRecommendation	Otorga permiso para obtener una recomendación específica dentro de AWS la organización de una organización. Esta API solo admite recomendaciones priorizadas	Lectura			
GetRecommendation	Concede permiso para obtener una recomendación específica	Lectura			
IncludeCheckItems [solo permiso]	Otorga permiso para incluir recomendaciones para las comprobaciones AWS de Trusted Advisor	Escritura	checks*		
ListAccountsForParent [solo permiso]	Otorga permiso para ver, en la consola de Trusted Advisor, todas las cuentas de una AWS organización incluidas en una raíz o unidad organizativa (OU)	Lectura			
ListChecks	Concede permiso para enumerar un conjunto de cheques filtrable	Enumeración			
ListEngagementCommunications	Concede permiso para ver todas las comunicaciones de una interacción	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListEngagementTypes	Concede permiso para ver todos los tipos de interacción	Lectura			
ListEngagements	Concede permiso para ver todas las interacciones	Lectura			
ListOrganizationRecommendationAccounts	Otorga permiso para enumerar las cuentas que poseen los recursos para una recomendación agregada de AWS la organización. Esta API solo admite recomendaciones priorizadas	Enumeración			
ListOrganizationRecommendationResources	Otorga permiso para incluir los recursos de una recomendación dentro de una AWS organización. Esta API solo admite recomendaciones priorizadas	Enumeración			
ListOrganizationRecommendations	Otorga permiso para incluir un conjunto filtrable de recomendaciones dentro de una AWS organización. Esta API solo admite recomendaciones priorizadas	Enumeración			
ListOrganizationalUnitsForParent [solo permiso]	Otorga permiso para ver, en la consola de Trusted Advisor, todas las unidades organizativas (OUs) de una unidad organizativa principal o raíz	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRecommendationResources	Concede permiso para enumerar recursos de una recomendación	Enumeración			
ListRecommendations	Concede permiso para enumerar un conjunto filtrable de recomendaciones	Enumeración			
ListRoots [solo permiso]	Otorga permiso para ver, en la consola de Trusted Advisor, todas las raíces definidas en una AWS organización	Lectura			
RefreshCheck	Otorga permiso para actualizar un cheque AWS de Trusted Advisor	Escritura	checks*		
SetAccountAccess [solo permiso]	Otorga permiso para activar o desactivar AWS Trusted Advisor para la cuenta	Escritura			
SetOrganizationAccess [solo permiso]	Otorga permiso para activar la función de visualización de la organización para AWS Trusted Advisor	Escritura			
UpdateEngagement	Concede permiso para actualizar el detalle de una interacción	Escritura			
UpdateEngagementStatus	Concede permiso para actualizar el estado de una interacción	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateNotificationConfigurations	Concede permiso para crear o actualizar las preferencias de notificación por correo electrónico para Trusted Advisor Priority	Escritura			
UpdateNotificationPreferences [solo permiso]	Otorga permiso para actualizar las preferencias de notificación de AWS Trusted Advisor	Escritura			
UpdateOrganizationRecommendationLifecycle	Otorga permiso para actualizar el ciclo de vida de una recomendación dentro de una AWS organización. Esta API solo admite recomendaciones priorizadas	Escritura			
UpdateRecommendationLifecycle	Concede permiso para actualizar el ciclo de vida de una recomendación. Esta API solo admite recomendaciones priorizadas	Escritura			
UpdateRiskStatus	Otorga permiso para actualizar el estado de riesgo en AWS Trusted Advisor Priority	Escritura			

Tipos de recursos definidos por AWS Trusted Advisor

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

> **Note**
>
> El ARN del tipo de recurso de las comprobaciones no debe incluir una región. En el formato, en lugar de "${Region}", utilice un "*"; de lo contrario, la política no funcionará correctamente.

Tipos de recurso	ARN	Claves de condición
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

Claves de condición para AWS Trusted Advisor

Trusted Advisor no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Notificaciones de usuario de AWS

AWS Las notificaciones de usuario (prefijo de servicio:`notifications`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Notificaciones de usuario de AWS
- Tipos de recursos definidos por Notificaciones de usuario de AWS
- Claves de condición para Notificaciones de usuario de AWS

Acciones definidas por Notificaciones de usuario de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateChannel	Otorga permiso para asociar un canal nuevo a un canal concreto NotificationConfiguration	Escritura	NotificationConfiguration*		
AssociateManagedNotificationAccountContact	Otorga permiso para asociar un contacto de la cuenta a una configuración de notificaciones gestionadas concreta	Escritura	ManagedNotificationConfiguration*		
AssociateManagedNotificatio	Otorga permiso para asociar un canal a una configuración de notificaciones gestionadas concreta	Escritura	ManagedNotificationConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
nAdditionalChannel					
CreateEventRule	Otorga permiso para crear uno nuevo EventRule y lo asocia a NotificationConfiguration	Escritura			
CreateNotificationConfiguration	Otorga permiso para crear un NotificationConfiguration	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEventRule	Otorga permiso para eliminar un EventRule	Escritura	EventRule*		
DeleteNotificationConfiguration	Otorga permiso para eliminar un NotificationConfiguration	Escritura	NotificationConfiguration*		
DeregisterNotificationHub	Otorga permiso para anular el registro de un NotificationHub	Escritura			
DisableNotificationsAccessForOrganization	Otorga permiso para deshabilitar Service Trust for AWS User Notifications	Escritura			organizations:DisableAWSServiceAccess
DisassociateChannel	Otorga permiso para eliminar un canal de un NotificationConfiguration	Escritura	NotificationConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateManagedNotificationAccountContact	Otorga permiso para eliminar un contacto de una cuenta de una configuración de notificaciones gestionadas	Escritura	ManagedNotificationConfiguration*		
DisassociateManagedNotificationAdditionalChannel	Otorga permiso para eliminar un canal de una configuración de notificaciones gestionadas	Escritura	ManagedNotificationConfiguration*		
EnableNotificationsAccessForOrganization	Otorga permiso para habilitar la confianza en el servicio para las notificaciones AWS de los usuarios	Escritura			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
GetEventRule	Otorga permiso para obtener un EventRule	Lectura	EventRule*		
GetFeatureOptInStatus [solo permiso]	Otorga permiso para leer el estado de suscripción de una función del Servicio de notificaciones al AWS usuario	Lectura			
GetManagedNotificationChildEvent	Otorga permiso para obtener una notificación gestionada (evento secundario)	Lectura	ManagedNotificationChildEvent*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetManagedNotificationConfiguration	Otorga permiso para obtener una configuración de notificaciones gestionadas	Lectura	ManagedNotificationConfiguration*		
GetManagedNotificationEvent	Otorga permiso para obtener una Gestionada NotificationEvent	Lectura	ManagedNotificationEvent*		
GetNotificationConfiguration	Otorga permiso para obtener un NotificationConfiguration	Lectura	NotificationConfiguration*		
GetNotificationEvent	Otorga permiso para obtener un NotificationEvent	Lectura	NotificationEvent*		
GetNotificationsAccessForOrganization	Otorga permiso para leer Service Trust for AWS User Notifications	Lectura			
ListChannels	Otorga permiso para enumerar los canales por NotificationConfiguration	Enumeración	NotificationConfiguration*		
ListEventRules	Otorga permiso para publicar EventRules	Enumeración			
ListManagedNotificationChannelAssociations	Otorga permiso para enumerar los contactos y canales de la cuenta asociados a una configuración de notificaciones gestionadas	Enumeración	ManagedNotificationConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListManagedNotificationChildEvents	Otorga permiso para enumerar los eventos secundarios de Managed Notification	Enumeración			
ListManagedNotificationConfigurations	Otorga permiso para enumerar las configuraciones de notificaciones gestionadas	Enumeración			
ListManagedNotificationEvents	Otorga permiso para enumerar los eventos de notificación gestionados	Enumeración			
ListNotificationConfigurations	Otorga permiso para publicar NotificationConfigurations	Enumeración			
ListNotificationEvents	Otorga permiso para publicar NotificationEvents	Enumeración			
ListNotificationHubs	Otorga permiso para publicar NotificationHubs	Enumeración			
ListTagsForResource	Otorga permiso para obtener las etiquetas de un recurso	Enumeración			
PutFeatureOptInStatus [solo permiso]	Otorga permiso para actualizar el estado de suscripción de una función del Servicio de notificaciones al AWS usuario	Escritura			
RegisterNotificationHub	Otorga permiso para registrar un NotificationHub	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	NotificationConfiguration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	Otorga permiso para actualizar un EventRule	Escritura	EventRule*		
UpdateNotificationConfiguration	Otorga permiso para actualizar un NotificationConfiguration	Escritura	NotificationConfiguration*		

Tipos de recursos definidos por Notificaciones de usuario de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
EventRule	arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}/rule/${EventRuleId}	
NotificationConfiguration	arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}	aws:ResourceTag/${TagKey}
NotificationEvent	arn:${Partition}:notifications:${Region}:${Account}:configuration/${NotificationConfigurationId}/event/${NotificationEventId}	
ManagedNotificationChildEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}/child-event/${NotificationChildEventId}	
ManagedNotificationConfiguration	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}	
ManagedNotificationEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}	

Claves de condición para Notificaciones de usuario de AWS

AWS Las notificaciones de usuario definen las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para Contactos de notificaciones de usuario de AWS

AWS Los contactos de notificaciones de usuario (prefijo de servicio:`notifications-contacts`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Contactos de notificaciones de usuario de AWS
- Tipos de recursos definidos por Contactos de notificaciones de usuario de AWS
- Claves de condición para Contactos de notificaciones de usuario de AWS

Acciones definidas por Contactos de notificaciones de usuario de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ActivateEmailContact	Otorga permiso para activar el contacto de correo electrónico asociado al ARN dado si el código proporcionado es válido	Escritura	EmailContactResource*		
CreateEmailContact	Concede permiso para crear un contacto de correo electrónico	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEmailContact	Concede permiso para eliminar un contacto de correo electrónico asociado con el ARN dado	Escritura	EmailContactResource*		
GetEmailContact	Concede permiso para obtener un contacto de correo	Lectura	EmailContactResource*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	electrónico asociado con el ARN dado				
ListEmailContacts	Concede permiso para enumerar los contactos de correo electrónico	Enumeración			
ListTagsForResource	Otorga permiso para obtener las etiquetas de un recurso	Lectura			
SendActivationCode	Otorga permiso para enviar un enlace de activación al correo electrónico asociado al ARN dado	Escritura	EmailContactResource*		
TagResource	Concede permiso para etiquetar un recurso	Etiquetado	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar etiquetas de un recurso	Etiquetado	EmailContactResource*		
				aws:TagKeys	

Tipos de recursos definidos por Contactos de notificaciones de usuario de AWS

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
EmailContactResource	`arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}`	aws:ResourceTag/${TagKey}

Claves de condición para Contactos de notificaciones de usuario de AWS

AWS User Notifications Contacts define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS User Subscriptions

AWS Las suscripciones de usuario (prefijo de servicio:`user-subscriptions`) proporcionan los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS User Subscriptions
- Tipos de recursos definidos por AWS User Subscriptions
- Claves de condición para AWS User Subscriptions

Acciones definidas por AWS User Subscriptions

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateClaim	Concede permiso para crear una reclamación de suscripción de usuario	Escritura		user-subscriptions:CreateForSelf	
DeleteClaim	Concede permiso para eliminar una reclamación de suscripción de usuario	Escritura			
ListApplicationClaims	Concede permiso para enumerar todas las reclamaciones de suscripción de usuario para la aplicación	Enumeración			
ListClaims	Concede permiso para enumerar todas las reclamaciones de suscripción de usuario	Enumeración			
ListUserSubscriptions	Concede permiso para enumerar todas las suscripciones de usuario	Enumeración			
UpdateClaim	Concede permiso para actualizar una reclamación de suscripción de usuario	Escritura			

Tipos de recursos definidos por AWS User Subscriptions

AWS Las suscripciones de usuarios no admiten la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a AWS User Subscriptions, especifique `"Resource": "*"` en la política.

Claves de condición para AWS User Subscriptions

AWS Las suscripciones de usuario definen las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
user-subscriptions:CreateForSelf	Filtra el acceso al permitir únicamente la creación de solicitudes de suscripción de usuario para la persona que llama	Bool

Acciones, recursos y claves de condición para Acceso verificado de AWS

AWS El acceso verificado (prefijo de servicio:`verified-access`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Acceso verificado de AWS
- Tipos de recurso definidos por Acceso verificado de AWS
- Claves de condición para Acceso verificado de AWS

Acciones definidas por Acceso verificado de AWS

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVerifiedAccess [solo permiso]	Concede permiso para crear una instancia de Acceso verificado	Escritura			

Tipos de recurso definidos por Acceso verificado de AWS

AWS Verified Access no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a Acceso verificado de AWS , especifique `"Resource": "*"` en la política.

Claves de condición para Acceso verificado de AWS

Acceso verificado no tiene claves de contexto específicas del servicio que se puedan utilizar en el elemento `Condition` de las instrucciones de política. Para ver la lista de claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición para Amazon Verified Permissions

Amazon Verified Permissions (prefijo de servicio: `verifiedpermissions`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon Verified Permissions
- Tipos de recurso definidos por Amazon Verified Permissions
- Claves de condición para Amazon Verified Permissions

Acciones definidas por Amazon Verified Permissions

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIdentitySource	Concede permiso para crear una referencia a un proveedor de identidades (IdP) externo compatible con el protocolo de autenticación OpenID Connect (OIDC), como Amazon Cognito	Escritura	policy-store*		
CreatePolicy	Concede permiso para crear una política de Cedar y guardarla en el almacén de políticas especificado	Escritura	policy-store*		
CreatePolicyStore	Concede permiso para crear una política de Cedar y	Escritura		aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	guardarla en el almacén de políticas especificado			aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyTemplate	Concede permiso para crear una plantilla de política	Escritura	policy-store*		
DeleteIdentitySource	Concede permiso para eliminar un origen de identidad que hace referencia a un proveedor de identidades (IdP) como Amazon Cognito	Escritura	policy-store*		
DeletePolicy	Concede permiso para eliminar la política especificada del almacén de políticas	Escritura	policy-store*		
DeletePolicyStore	Concede permiso para eliminar el almacén de políticas especificado	Escritura	policy-store*		
DeletePolicyTemplate	Concede permiso para eliminar la plantilla de política especificada del almacén de políticas	Escritura	policy-store*		
GetIdentitySource	Concede permiso para recuperar los detalles sobre el origen de identidad especificado	Lectura	policy-store*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetPolicy	Concede permiso para recuperar la información sobre la política especificada	Lectura	policy-store*		
GetPolicyStore	Concede permiso para recuperar detalles sobre un almacén de políticas	Lectura	policy-store*		verifiedpermissions:ListTagsForResource
GetPolicyTemplate	Concede permiso para recuperar los detalles de la plantilla de política especificada en el almacén de políticas especificado	Lectura	policy-store*		
GetSchema	Concede permiso para recuperar los detalles del esquema especificado en el almacén de políticas especificado	Lectura	policy-store*		
IsAuthorized	Concede permiso para tomar una decisión de autorización sobre una solicitud de servicio descrita en los parámetros	Lectura	policy-store*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
IsAuthorizedWithToken	Concede permiso para tomar una decisión de autorización sobre una solicitud de servicio descrita en los parámetros. La entidad principal de esta solicitud proviene de un origen de identidad externo	Lectura	policy-store*		
ListIdentitySources	Concede permiso para devolver una lista paginada de todos los orígenes de identidad definidos en el almacén de políticas especificado	Enumeración	policy-store*		
ListPolicies	Concede permiso para devolver una lista paginada de todas las políticas almacenadas en el almacén de políticas especificado	Enumeración	policy-store*		
ListPolicyStores	Concede permiso para devolver una lista paginada de todos los almacenes de políticas de la cuenta de Amazon Web Services que hace la llamada	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListPolicyTemplates	Concede permiso para devolver una lista paginada de todas las plantillas de políticas del almacén de políticas especificado	Enumeración	policy-store*		
ListTagsForResource	Otorga permiso para ver una lista de etiquetas de recursos del almacén de políticas especificado	Lectura	policy-store*		
PutSchema	Concede permiso para crear o actualizar el esquema de políticas en el almacén de políticas especificado	Escritura	policy-store*		
TagResource	Otorga permiso para añadir etiquetas al almacén de políticas especificado	Etiquetado	policy-store*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas del almacén de políticas especificado	Etiquetado	policy-store*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIdentitySource	Concede permiso para actualizar el origen de identidad especificado para usar un nuevo origen de proveedor de identidades (IdP) o para cambiar la asignación de identidades del IdP a un tipo de entidad principal diferente	Escritura	policy-store*		
UpdatePolicy	Concede permiso para modificar la política estática de Cedar especificada en el almacén de políticas especificado	Escritura	policy-store*		
UpdatePolicyStore	Concede permiso para modificar la configuración de validación de un almacén de políticas	Escritura	policy-store*		
UpdatePolicyTemplate	Concede permiso para actualizar la plantilla de política especificada	Escritura	policy-store*		

Tipos de recurso definidos por Amazon Verified Permissions

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se

muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
policy-store	`arn:${Partition}:verifiedpermissions::${Account}:policy-store/${PolicyStoreId}`	aws:ResourceTag/${TagKey}

Claves de condición para Amazon Verified Permissions

Amazon Verified Permissions define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante una clave de etiqueta y un par de valores permitidos en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por par de clave y valor de etiqueta de un recurso	Cadena
aws:TagKeys	Filtra el acceso mediante una lista de claves de etiqueta permitidas en la solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon VPC Lattice

Amazon VPC Lattice (prefijo de servicio: `vpc-lattice`) proporciona las siguientes acciones, recursos y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon VPC Lattice
- Tipos de recurso definidos por Amazon VPC Lattice
- Claves de condición para Amazon VPC Lattice

Acciones definidas por Amazon VPC Lattice

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar

la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate ViaAWSService [solo permiso]	Otorga permiso para asociar una configuración de recursos a través de cualquier red gestionada por AWS servicios	Administración de permisos			
Associate ViaAWSService-EventsAndStat	Otorga permiso para asociar una configuración de recursos a través de las redes de servicios Amazon EventBridge y AWS Step Functions	Administración de permisos			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
es [solo permiso]					
CreateAccessLogSubscription	Otorga permiso para crear una suscripción de registro de acceso	Escritura	AccessLogSubscription*		logs:CreateLogDelivery logs:GetLogDelivery
			ResourceConfiguration		
			Service		
			ServiceNetwork		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateListener	Otorga permiso para crear un oyente	Escritura	Listener*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns	
CreateResourceConfiguration	Otorga permiso para crear una configuración de recursos	Escritura	ResourceConfiguration		
			ResourceGateway		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateResourceGateway	Otorga permiso para crear una puerta de enlace de recursos	Escritura	ResourceGateway*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId	
CreateRule	Concede permiso para crear una regla	Escritura	Rule*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateService	Otorga permiso para crear un servicio.	Escritura	Service*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType	
CreateServiceNetwork	Otorga permiso para crear una red de servicios	Escritura	ServiceNetwork*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType	
CreateServiceNetworkResourceAssociation	Otorga permiso para crear una asociación entre una red de servicios y un recurso	Escritura	ResourceConfiguration*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ServiceNetwork*		
			ServiceNetworkResourceAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn	
CreateServiceNetworkServiceAssociation	Otorga permiso para crear una red de servicios y una asociación de servicios	Escritura	Service*		
			ServiceNetwork*		
			ServiceNetworkServiceAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
CreateServiceNetworkVpcAssociation	Otorga permiso para crear una red de servicios y una asociación de VPC	Escritura	ServiceNetwork*		ec2:DescribeVpcs
			ServiceNetworkVpcAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
CreateServiceNetworkVpcEndpointAssociation [solo permiso]	Concede permiso para crear una asociación entre una red de servicio y un punto final de VPC	Administración de permisos			
CreateTargetGroup	Concede permiso para crear un grupo de destino.	Escritura	TargetGroup*		iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId	
DeleteAccessLogSubscription	Otorga permiso para eliminar una suscripción de registro de acceso	Escritura	AccessLogSubscription*		logs:DeleteLogDelivery logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
DeleteAuthPolicy	Otorga permiso para eliminar una política de autenticación	Administración de permisos	Service		
			ServiceNetwork		
DeleteListener	Otorga permiso para eliminar un oyente	Escritura	Listener*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourceConfiguration	Otorga permiso para eliminar una configuración de recursos	Escritura	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteResourceEndpointAssociation	Otorga permiso para eliminar una asociación de puntos finales de recursos	Escritura	ResourceEndpointAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteResourceGateway	Otorga permiso para eliminar una puerta de enlace de recursos	Escritura	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Concede permiso para eliminar una política de recursos.	Escritura	ResourceConfiguration		
			Service		
			ServiceNetwork		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRule	Otorga permiso para eliminar una regla	Escritura	Rule*		
				aws:ResourceTag/${TagKey}	
DeleteService	Otorga permiso para eliminar un servicio.	Escritura	Service*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetwork	Otorga permiso para eliminar una red de servicios	Escritura	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkResourceAssociation	Otorga permiso para eliminar la asociación entre una red de servicios y un recurso	Escritura	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkServiceAssociation	Otorga permiso para eliminar una asociación de servicios de red de servicios	Escritura	ServiceNetworkServiceAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
DeleteServiceNetworkVpcAssociation	Otorga permiso para eliminar una red de servicios y una asociación de VPC	Escritura	ServiceNetworkVpcAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
DeleteTargetGroup	Otorga permiso para eliminar un grupo de destino	Escritura	TargetGroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeregisterTargets	Otorga permiso para dar de baja destinos de un grupo de destinos	Escritura	TargetGroup*		
GetAccessLogSubscription	Otorga permiso para obtener información sobre una suscripción de registro de acceso	Lectura	AccessLogSubscription*		logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
GetAuthPolicy	Otorga permiso para obtener información sobre una política de autenticación	Lectura	Service		
			ServiceNetwork		
GetListener	Otorga permiso para obtener información sobre un oyente	Lectura	Listener*		
				aws:ResourceTag/${TagKey}	
GetResourceConfiguration	Otorga permiso para obtener información sobre la configuración de un recurso	Lectura	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetResourceGateway	Otorga permiso para obtener información sobre una pasarela de recursos	Lectura	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Otorga permiso para obtener información sobre una política de recursos	Lectura	ResourceConfiguration		
			Service		
			ServiceNetwork		
GetRule	Otorga permiso para obtener información sobre una regla	Lectura	Rule*		
				aws:ResourceTag/${TagKey}	
GetService	Otorga permiso para obtener información sobre un servicio	Lectura	Service*		
				aws:ResourceTag/${TagKey}	
GetServiceNetwork	Otorga permiso para obtener información sobre una red de servicios	Lectura	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetServiceNetworkResourceAssociation	Otorga permiso para obtener información sobre una asociación entre una red de servicios y la configuración de recursos	Lectura	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkServiceAssociation	Otorga permiso para obtener información sobre una red de servicios y una asociación de servicios	Lectura	ServiceNetworkServiceAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
GetServiceNetworkVpcAssociation	Otorga permiso para obtener información sobre una red de servicios y una asociación de VPC	Lectura	ServiceNetworkVpcAssociation*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
GetTargetGroup	Otorga permiso para obtener información sobre un grupo de destino	Lectura	TargetGroup*		
				aws:ResourceTag/${TagKey}	
ListAccessLogSubscriptions	Otorga permiso para enumerar algunas o todas las suscripciones de registro de acceso sobre una red de servicios o un servicio	Enumeración			
ListListeners	Otorga permiso para enumerar algunos o todos los oyentes	Enumeración			
ListResourceConfigurations	Otorga permiso para enumerar algunas o todas las configuraciones de recursos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourceEndpointAssociations	Otorga permiso para enumerar algunas o todas las asociaciones entre una configuración de recursos y un punto final de VPC	Enumeración		vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId	
ListResourceGateways	Otorga permiso para enumerar algunas o todas las pasarelas de recursos	Enumeración			
ListRules	Otorga permiso para enumerar algunas o todas las reglas	Enumeración			
ListServiceNetworkResourceAssociations	Otorga permiso para enumerar algunas o todas las asociaciones entre una red de servicios y la configuración de recursos	Enumeración			
ListServiceNetworkServiceAssociations	Otorga permiso para enumerar algunas o todas las redes de servicios y asociaciones servicios	Enumeración		vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListServiceNetworkVpcAssociations	Otorga permiso para enumerar algunas o todas las redes de servicios y asociaciones de VPC	Enumeración		vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
ListServiceNetworkVpcEndpointAssociations	Otorga permiso para enumerar algunas o todas las asociaciones entre una red de servicio y un punto final de VPC	Enumeración			
ListServiceNetworks	Otorga permiso para enumerar las redes de servicios propiedad de una cuenta de intermediario o compartidas con dicha cuenta	Enumeración			
ListServices	Otorga permiso para enumerar los servicios propiedad de una cuenta de intermediario o compartidos con dicha cuenta	Enumeración			
ListTagsForResource	Otorga permiso para enumerar etiquetas de un recurso vpc-lattice	Lectura			
ListTargetGroups	Otorga permiso para enumerar algunos o todos los grupos de destino	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTargets	Otorga permiso para enumerar algunos o todos los destinos de un grupo de destino	Enumeración	TargetGroup*		
PutAuthPolicy	Otorga permiso para crear o actualizar la política de autenticación de una red de servicios o de un servicio	Administración de permisos	Service		
			ServiceNetwork		
PutResourcePolicy	Otorga permiso para crear una política de recursos para una configuración de recursos, un servicio o una red de servicios	Escritura	ResourceConfiguration		
			Service		
			ServiceNetwork		
RegisterTargets	Otorga permiso para registrar destinos en un grupo de destino	Escritura	TargetGroup*		
TagResource	Otorga permiso para etiquetar un recurso vpc-lattice	Etiquetado	AccessLogSubscription		
			Listener		
			ResourceConfiguration		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para quitar la etiqueta de un recurso vpc-lattice	Etiquetado	AccessLogSubscription		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys	
UpdateAccessLogSubscription	Otorga permiso para actualizar una suscripción de registro de acceso	Escritura	AccessLogSubscription*		logs:GetLogDelivery logs:UpdateLogDelivery
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateListener	Otorga permiso para actualizar un oyente	Escritura	Listener*		
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateResourceConfiguration	Otorga permiso para actualizar una configuración de recursos	Escritura	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateResourceGateway	Otorga permiso para actualizar una puerta de enlace de recursos	Escritura	ResourceGateway*		
				aws:ResourceTag/${TagKey} vpc-lattice:SecurityGroupIds	
UpdateRule	Otorga permiso para actualizar una regla	Escritura	Rule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateService	Otorga permiso para actualizar un servicio.	Escritura	Service*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetwork	Otorga permiso para actualizar una red de servicios	Escritura	ServiceNetwork*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateServiceNetworkVpcAssociation	Otorga permiso para actualizar una red de servicios y una asociación de VPC	Escritura	ServiceNetworkVpcAssociation*		ec2:DescribeSecurityGroups ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
UpdateTargetGroup	Otorga permiso para actualizar un grupo de destino	Escritura	TargetGroup*		
				aws:ResourceTag/${TagKey}	

Tipos de recurso definidos por Amazon VPC Lattice

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
AccessLogSubscription	`arn:${Partition}:vpc-lattice:${Region}:${Account}:accesslogsubscription/${AccessLogSubscriptionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
Listener	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns
ResourceConfiguration	`arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceconfiguration/${ResourceConfigurationId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Tipos de recurso	ARN	Claves de condición
ResourceEndpointAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceendpointassociation/${ResourceEndpointAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId
ResourceGateway	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourcegateway/${ResourceGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:VpcId
Rule	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}/rule/${RuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns

Tipos de recurso	ARN	Claves de condición
Service	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType
ServiceNetwork	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetwork/${ServiceNetworkId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType
ServiceNetworkResourceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkresourceassociation/${ServiceNetworkResourceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn

Tipos de recurso	ARN	Claves de condición
ServiceNetworkServiceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkserviceassociation/${ServiceNetworkServiceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn
ServiceNetworkVpcAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkvpcassociation/${ServiceNetworkVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId
TargetGroup	arn:${Partition}:vpc-lattice:${Region}:${Account}:targetgroup/${TargetGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:VpcId

Claves de condición para Amazon VPC Lattice

Amazon VPC Lattice define las siguientes claves de condición que se pueden utilizar en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso según si hay pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso en función de la presencia de claves de etiqueta en la solicitud	ArrayOfString
vpc-lattice:AuthType	Filtra el acceso por el tipo de autenticación especificado en la solicitud	Cadena
vpc-lattice:Protocol	Filtra el acceso por el protocolo especificado en la solicitud	Cadena
vpc-lattice:ResourceConfigurationArn	Filtra el acceso por el ARN de una configuración de recursos	ARN
vpc-lattice:SecurityGroupIds	Filtra el acceso por parte IDs de los grupos de seguridad	ArrayOfString

Claves de condición	Descripción	Tipo
vpc-lattice:ServiceArn	Filtra el acceso por el ARN de un servicio	ARN
vpc-lattice:ServiceNetworkArn	Filtra el acceso por el ARN de una red de servicios	ARN
vpc-lattice:TargetGroupArns	Filtra el acceso por parte ARNs de los grupos objetivo	ArrayOfARN
vpc-lattice:VpcEndpointId	Filtra el acceso por el ID de un punto final de VPC	Cadena
vpc-lattice:VpcId	Filtra el acceso por el ID de una nube virtual privada (VPC)	Cadena

Acciones, recursos y claves de condición para Amazon VPC Lattice Services

Amazon VPC Lattice Services (prefijo de servicio: `vpc-lattice-svcs`) proporciona los siguientes recursos específicos del servicio, acciones y claves de contexto de condición para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon VPC Lattice Services

- Tipos de recursos definidos por Amazon VPC Lattice Services
- Claves de condición para Amazon VPC Lattice Services

Acciones definidas por Amazon VPC Lattice Services

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Connect	Concede permiso para establecer conexión con un servicio de VPC Lattice	Escritura	TCP Service*		
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Invoke	Otorga permiso para invocar un servicio de VPC Lattice	Escritura	Service*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount vpc-lattice-svcs:RequestHeader/${HeaderName} vpc-lattice-	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				svcs:RequestQueryString/${QueryStringKey}	

Tipos de recursos definidos por Amazon VPC Lattice Services

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/${RequestPath}`	
TCP Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}`	

Claves de condición para Amazon VPC Lattice Services

Amazon VPC Lattice Services define las siguientes claves de condición que pueden utilizarse en el elemento `Condition` de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
vpc-lattice-svcs:Port	Filtra el acceso por el puerto de destino al que se realiza la solicitud	Numérico
vpc-lattice-svcs:RequestHeader/${HeaderName}	Filtra el acceso por un par de nombre-valor de encabezado en los encabezados de la solicitud	Cadena
vpc-lattice-svcs:RequestMethod	Filtra el acceso por el método de la solicitud	Cadena
vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	Filtra el acceso por los pares de clave-valor de la cadena de consulta en la URL de la solicitud	ArrayOfString
vpc-lattice-svcs:ServiceArn	Filtra el acceso por el ARN del servicio que recibe la solicitud	ARN
vpc-lattice-svcs:ServiceNetworkArn	Filtra el acceso por el ARN de la red de servicios que recibe la solicitud	ARN
vpc-lattice-svcs:SourceVpc	Filtra el acceso por la VPC desde la que se realiza la solicitud	Cadena
vpc-lattice-svcs:S	Filtra el acceso por la cuenta propietaria de la VPC desde la que se realiza la solicitud	Cadena

Claves de condición	Descripción	Tipo
ourceVpcOwnerAccount		

Acciones, recursos y claves de condición para AWS WAF

AWS El WAF (prefijo de servicio:`waf`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS WAF
- Tipos de recursos definidos por AWS WAF
- Claves de condición para AWS WAF

Acciones definidas por AWS WAF

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateByteMatchSet	Otorga permiso para crear un ByteMatchSet	Escritura	bytematchset*		
CreateGeoMatchSet	Otorga permiso para crear un GeoMatchSet	Escritura	geomatchset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIPSet	Otorga permiso para crear un IPSet	Escritura	ipset*		
CreateRateBasedRule	Otorga permiso para crear un RateBasedRule para limitar el volumen de solicitudes desde una sola dirección IP	Escritura	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Otorga permiso para crear un RegexMatchSet	Escritura	regexmatchset*		
CreateRegexPatternSet	Otorga permiso para crear un RegexPatternSet	Escritura	regexpatternset*		
CreateRule	Concede permiso para crear una regla para filtrar solicitudes web	Escritura	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Otorga permiso para crear una RuleGroup, que es una colección de reglas predefinidas que puede usar en una WebACL	Escritura	rulegroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Otorga permiso para crear un SizeConstraintSet	Escritura	sizeconstraintset*		
CreateSqlInjectionMatchSet	Otorga permiso para crear un SqlInjectionMatchSet	Escritura	sqlinjectionmatchset*		
CreateWebACL	Concede permiso para crear una WebACL, que contiene reglas para filtrar solicitudes web	Administración de permisos	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Otorga permiso para crear una plantilla de ACL CloudFormation web en un bucket de S3 con el fin de migrar la ACL web de AWS WAF Classic a AWS WAF v2	Escritura	webacl*		s3:PutObject

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateXssMatchSet	Otorga permiso para crear una XssMatchSet, que se utiliza para detectar solicitudes que contienen ataques de secuencias de comandos entre sitios	Escritura	xssmatchset*		
DeleteByteMatchSet	Otorga permiso para eliminar un ByteMatchSet	Escritura	bytematchset*		
DeleteGeoMatchSet	Otorga permiso para eliminar un GeoMatchSet	Escritura	geomatchset*		
DeleteIPSet	Otorga permiso para eliminar un IPSet	Escritura	ipset*		
DeleteLoggingConfiguration	Otorga permiso para eliminarla LoggingConfiguration de una ACL web	Escritura	webacl*		
DeletePermissionPolicy	Concede permiso para eliminar una política de IAM de un grupo de reglas	Administración de permisos	rulegroup*		
DeleteRateBasedRule	Otorga permiso para eliminar un RateBasedRule	Escritura	ratebasedrule*		
DeleteRegexMatchSet	Otorga permiso para eliminar un RegexMatchSet	Escritura	regexmatchset*		
DeleteRegexPatternSet	Otorga permiso para eliminar un RegexPatternSet	Escritura	regexpatternset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRule	Concede permiso para eliminar una regla	Escritura	rule*		
DeleteRuleGroup	Otorga permiso para eliminar un RuleGroup	Escritura	rulegroup*		
DeleteSizeConstraintSet	Otorga permiso para eliminar un SizeConstraintSet	Escritura	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Otorga permiso para eliminar un SqlInjectionMatchSet	Escritura	sqlinjectionmatchset*		
DeleteWebACL	Concede permiso para eliminar una WebACL	Administración de permisos	webacl*		
DeleteXssMatchSet	Otorga permiso para eliminar un XssMatchSet	Escritura	xssmatchset*		
GetByteMatchSet	Otorga permiso para recuperar un ByteMatchSet	Lectura	bytematchset*		
GetChangeToken	Concede permiso para recuperar un token de cambio para utilizarlo en las solicitudes de creación, actualización y eliminación	Read			
GetChangeTokenStatus	Concede permiso para recuperar el estado de un token de cambio	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGeoMatchSet	Otorga permiso para recuperar un GeoMatchSet	Lectura	geomatchset*		
GetIPSet	Otorga permiso para recuperar un IPSet	Lectura	ipset*		
GetLoggingConfiguration	Otorga permiso LoggingConfiguration para recuperar una ACL web	Lectura	webacl*		
GetPermissionPolicy	Concede permiso para recuperar una política de IAM para un grupo de reglas	Lectura	rulegroup*		
GetRateBasedRule	Otorga permiso para recuperar un RateBasedRule	Lectura	ratebasedrule*		
GetRateBasedRuleManagedKeys	Otorga permiso para recuperar la matriz de direcciones IP que está bloqueando actualmente un RateBasedRule	Lectura	ratebasedrule*		
GetRegexMatchSet	Otorga permiso para recuperar un RegexMatchSet	Lectura	regexmatchset*		
GetRegexPatternSet	Otorga permiso para recuperar un RegexPatternSet	Lectura	regexpatternset*		
GetRule	Concede permiso para recuperar una regla	Lectura	rule*		
GetRuleGroup	Otorga permiso para recuperar un RuleGroup	Lectura	rulegroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetSampledRequests	Concede permiso para recuperar información detallada sobre un conjunto de ejemplo de solicitudes web	Lectura	webacl		
GetSizeConstraintSet	Otorga permiso para recuperar un SizeConstraintSet	Lectura	sizeconstraintset*		
GetSqlInjectionMatchSet	Otorga permiso para recuperar un SqlInjectionMatchSet	Lectura	sqlinjectionmatchset*		
GetWebACL	Concede permisos para recuperar una WebACL	Lectura	webacl*		
GetXssMatchSet	Otorga permiso para recuperar un XssMatchSet	Lectura	xssmatchset*		
ListActivatedRulesInRuleGroup	Otorga permiso para recuperar una matriz de ActivatedRule objetos	Enumeración			
ListByteMatchSets	Otorga permiso para recuperar una matriz de ByteMatchSetSummary objetos	Enumeración			
ListGeoMatchSets	Otorga permiso para recuperar una matriz de GeoMatchSetSummary objetos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListIPSets	Otorga permiso para recuperar una matriz de objetos de IPSet Summary	Enumeración			
ListLoggingConfigurations	Otorga permiso para recuperar una matriz de LoggingConfiguration objetos	Enumeración			
ListRateBasedRules	Otorga permiso para recuperar una matriz de RuleSummary objetos	Enumeración			
ListRegexMatchSets	Otorga permiso para recuperar una matriz de RegexMatchSetSummary objetos	Enumeración			
ListRegexPatternSets	Otorga permiso para recuperar una matriz de RegexPatternSetSummary objetos	Enumeración			
ListRuleGroups	Otorga permiso para recuperar una matriz de RuleGroup objetos	Enumeración			
ListRules	Otorga permiso para recuperar una matriz de RuleSummary objetos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSizeConstraintSets	Otorga permiso para recuperar una matriz de SizeConstraintSetSummary objetos	Enumeración			
ListSqlInjectionMatchSets	Otorga permiso para recuperar una matriz de SqlInjectionMatchSet objetos	Enumeración			
ListSubscribedRuleGroups	Otorga permiso para recuperar una matriz de RuleGroup objetos a la que está suscrito	Enumeración			
ListTagsForResource	Concede permiso para recuperar las etiquetas de un recurso.	Lectura	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Otorga permiso para recuperar una matriz de objetos web ACLSummary	Enumeración			
ListXssMatchSets	Otorga permiso para recuperar una matriz de XssMatchSet objetos	Enumeración			
PutLoggingConfiguration	Otorga permiso para asociar a a una ACL web específica LoggingConfiguration	Escritura	webacl*		iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutPermissionPolicy	Concede permiso para adjuntar una política de IAM a un grupo de reglas, a fin de compartir el grupo de reglas entre cuentas	Permissions management	rulegroup *		
TagResource	Concede permiso para agregar una etiqueta a un recurso	Etiquetado	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una etiqueta de un recurso	Etiquetado	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateByteMatchSet	Otorga permiso para insertar o eliminar ByteMatchTuple objetos en una ByteMatchSet	Escritura	bytematchset*		
UpdateGeoMatchSet	Otorga permiso para insertar o eliminar GeoMatchConstraint objetos en un GeoMatchSet	Escritura	geomatchset*		
UpdateIPSet	Otorga permiso para insertar o eliminar objetos IPSet descriptores en un IPSet	Escritura	ipset*		
UpdateRateBasedRule	Concede permiso para modificar una regla basada en tasas	Escritura	ratebasedrule*		
UpdateRegexMatchSet	Otorga permiso para insertar o eliminar RegexMatchTuple objetos en un RegexMatchSet	Escritura	regexmatchset*		
UpdateRegexPatternSet	Otorga permiso para insertar o eliminar RegexPatternStrings en un RegexPatternSet	Escritura	regexpatternset*		
UpdateRule	Concede permiso para modificar una regla	Escritura	rule*		
UpdateRuleGroup	Otorga permiso para insertar o eliminar ActivatedRule objetos en un RuleGroup	Escritura	rulegroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSizeConstraintSet	Otorga permiso para insertar o eliminar SizeConstraint objetos en un SizeConstraintSet	Escritura	sizeconstraintset*		
UpdateSqlInjectionMatchSet	Otorga permiso para insertar o eliminar SqlInjectionMatchTuple objetos en un SqlInjectionMatchSet	Escritura	sqlinjectionmatchset*		
UpdateWebACL	Otorga permiso para insertar o eliminar ActivatedRule objetos en una WebACL	Administración de permisos	webacl*		
UpdateXssMatchSet	Otorga permiso para insertar o eliminar XssMatchTuple objetos en una XssMatchSet	Escritura	xssmatchset*		

Tipos de recursos definidos por AWS WAF

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
bytematchset	`arn:${Partition}:waf::${Account}:bytematchset/${Id}`	

Tipos de recurso	ARN	Claves de condición
ipset	arn:${Partition}:waf::${Account}:ipset/${Id}	
ratebasedrule	arn:${Partition}:waf::${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf::${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf::${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf::${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf::${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf::${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf::${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf::${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf::${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf::${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

Claves de condición para AWS WAF

AWS El WAF define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función del conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de etiquetas obligatorias en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS WAF Regional

AWS WAF Regional (prefijo de servicio:`waf-regional`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS WAF Regional
- Tipos de recursos definidos por AWS WAF Regional
- Claves de condición para AWS WAF Regional

Acciones definidas por AWS WAF Regional

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos

(*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateWebACL	Concede permiso para asociar una ACL web a un recurso	Escritura	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	Otorga permiso para crear un ByteMatchSet	Escritura	bytematchset*		
CreateGeoMatchSet	Otorga permiso para crear un GeoMatchSet	Escritura	geomatchset*		
CreateIPSet	Otorga permiso para crear un IPSet	Escritura	ipset*		
CreateRateBasedRule	Otorga permiso para crear un RateBasedRule	Escritura	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Otorga permiso para crear un RegexMatchSet	Escritura	regexmatchset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRegexPatternSet	Otorga permiso para crear un RegexPatternSet	Escritura	regexpatternset*		
CreateRule	Concede permiso para crear una regla	Escritura	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Otorga permiso para crear un RuleGroup	Escritura	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Otorga permiso para crear un SizeConstraintSet	Escritura	sizeconstraintset*		
CreateSqlInjectionMatchSet	Otorga permiso para crear un SqlInjectionMatchSet	Escritura	sqlinjectionmatchset*		
CreateWebACL	Concede permiso para crear una WebACL	Administración de permisos	webacl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Otorga permiso para crear una plantilla de ACL CloudFormation web en un bucket de S3 con el fin de migrar la ACL web de AWS WAF Classic a AWS WAF v2	Escritura	webacl*		s3:PutObject
CreateXssMatchSet	Otorga permiso para crear una XssMatchSet	Escritura	xssmatchset*		
DeleteByteMatchSet	Otorga permiso para eliminar un ByteMatchSet	Escritura	bytematchset*		
DeleteGeoMatchSet	Otorga permiso para eliminar un GeoMatchSet	Escritura	geomatchset*		
DeleteIPSet	Otorga permiso para eliminar un IPSet	Escritura	ipset*		
DeleteLoggingConfiguration	Otorga permiso para eliminar una ACL LoggingConfiguration de una web	Escritura	webacl*		
DeletePermissionPolicy	Concede permiso para eliminar una política de IAM de un grupo de reglas	Administración de permisos	rulegroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteRateBasedRule	Otorga permiso para eliminar un RateBasedRule	Escritura	ratebasedrule*		
DeleteRegexMatchSet	Otorga permiso para eliminar un RegexMatchSet	Escritura	regexmatchset*		
DeleteRegexPatternSet	Otorga permiso para eliminar un RegexPatternSet	Escritura	regexpatternset*		
DeleteRule	Concede permiso para eliminar una regla	Escritura	rule*		
DeleteRuleGroup	Otorga permiso para eliminar un RuleGroup	Escritura	rulegroup*		
DeleteSizeConstraintSet	Otorga permiso para eliminar un SizeConstraintSet	Escritura	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Otorga permiso para eliminar un SqlInjectionMatchSet	Escritura	sqlinjectionmatchset*		
DeleteWebACL	Concede permiso para eliminar una WebACL	Administración de permisos	webacl*		
DeleteXssMatchSet	Otorga permiso para eliminar un XssMatchSet	Escritura	xssmatchset*		
DisassociateWebACL	Concede permiso para eliminar una asociación entre una ACL web y un recurso	Escritura	loadbalancer/app/*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetByteMatchSet	Otorga permiso para recuperar un ByteMatchSet	Lectura	bytematchset*		
GetChangeToken	Concede permiso para recuperar un token de cambio para utilizarlo en las solicitudes de creación, actualización y eliminación	Read			
GetChangeTokenStatus	Concede permiso para recuperar el estado de un token de cambio	Lectura			
GetGeoMatchSet	Otorga permiso para recuperar un GeoMatchSet	Lectura	geomatchset*		
GetIPSet	Otorga permiso para recuperar un IPSet	Lectura	ipset*		
GetLoggingConfiguration	Otorga permiso para recuperar un LoggingConfiguration	Lectura	webacl*		
GetPermissionPolicy	Otorga permiso para recuperar una política de IAM adjunta a un RuleGroup	Lectura	rulegroup*		
GetRateBasedRule	Otorga permiso para recuperar un RateBasedRule	Lectura	ratebasedrule*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRateBasedRuleManagedKeys	Otorga permiso para recuperar la matriz de direcciones IP que está bloqueando actualmente un RateBasedRule	Lectura	ratebasedrule*		
GetRegexMatchSet	Otorga permiso para recuperar un RegexMatchSet	Lectura	regexmatchset*		
GetRegexPatternSet	Otorga permiso para recuperar un RegexPatternSet	Lectura	regexpatternset*		
GetRule	Concede permiso para recuperar una regla	Lectura	rule*		
GetRuleGroup	Otorga permiso para recuperar un RuleGroup	Lectura	rulegroup*		
GetSampledRequests	Concede permiso para recuperar información detallada de un conjunto de ejemplo de solicitudes web	Lectura	webacl		
GetSizeConstraintSet	Otorga permiso para recuperar un SizeConstraintSet	Lectura	sizeconstraintset*		
GetSqlInjectionMatchSet	Otorga permiso para recuperar un SqlInjectionMatchSet	Lectura	sqlinjectionmatchset*		
GetWebACL	Concede permisos para recuperar una WebACL	Read	webacl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetWebACLForResource	Concede permiso para recuperar una WebACL asociada a un recurso especificado	Lectura	loadbalancer/app/*		
GetXssMatchSet	Otorga permiso para recuperar un XssMatchSet	Lectura	xssmatchset*		
ListActivatedRulesInRuleGroup	Otorga permiso para recuperar una matriz de ActivatedRule objetos	Enumeración			
ListByteMatchSets	Otorga permiso para recuperar una matriz de ByteMatchSetSummary objetos	Enumeración			
ListGeoMatchSets	Otorga permiso para recuperar una matriz de GeoMatchSetSummary objetos	Enumeración			
ListIPSets	Otorga permiso para recuperar una matriz de objetos de IPSet Summary	Enumeración			
ListLoggingConfigurations	Otorga permiso para recuperar una matriz de LoggingConfiguration objetos	Enumeración			
ListRateBasedRules	Otorga permiso para recuperar una matriz de RuleSummary objetos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRegexMatchSets	Otorga permiso para recuperar una matriz de RegexMatchSetSummary objetos	Enumeración			
ListRegexPatternSets	Otorga permiso para recuperar una matriz de RegexPatternSetSummary objetos	Enumeración			
ListResourcesForWebACL	Concede permiso para recuperar una matriz de recursos asociados a una WebACL especificada	Enumeración	webacl*		
ListRuleGroups	Otorga permiso para recuperar una matriz de RuleGroup objetos	Enumeración			
ListRules	Otorga permiso para recuperar una matriz de RuleSummary objetos	Enumeración			
ListSizeConstraintSets	Otorga permiso para recuperar una matriz de SizeConstraintSetSummary objetos	Enumeración			
ListSqlInjectionMatchSets	Otorga permiso para recuperar una matriz de SqlInjectionMatchSet objetos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSubscribedRuleGroups	Otorga permiso para recuperar una matriz de RuleGroup objetos a la que está suscrito	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Otorga permiso para recuperar una matriz de objetos web ACLSummary	Enumeración			
ListXssMatchSets	Otorga permiso para recuperar una matriz de XssMatchSet objetos	Enumeración			
PutLoggingConfiguration	Otorga permiso para asociar a a una ACL web LoggingConfiguration	Escritura	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	Concede permiso para adjuntar una política de IAM a un grupo de reglas especificado, a fin de admitir el uso compartido de grupos de reglas entre cuentas	Permissions management	rulegroup*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Concede permiso para agregar una etiqueta a un recurso	Etiquetado	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una etiqueta de un recurso	Etiquetado	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	Otorga permiso para insertar o eliminar ByteMatchTuple objetos en un ByteMatchSet	Escritura	bytematchset*		
UpdateGeoMatchSet	Otorga permiso para insertar o eliminar GeoMatchConstraint objetos en un GeoMatchSet	Escritura	geomatchset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIPSet	Otorga permiso para insertar o eliminar objetos IPSet descriptores en un IPSet	Escritura	ipset*		
UpdateRateBasedRule	Otorga permiso para insertar o eliminar objetos predicados en una regla basada en la tasa y actualizarlos RateLimit en la regla	Escritura	ratebasedrule*		
UpdateRegexMatchSet	Otorga permiso para insertar o eliminar RegexMatchTuple objetos en un RegexMatchSet	Escritura	regexmatchset*		
UpdateRegexPatternSet	Otorga permiso para insertar o eliminar RegexPatternStrings en un RegexPatternSet	Escritura	regexpatternset*		
UpdateRule	Concede permiso para insertar o eliminar objetos de predicado en una regla	Escritura	rule*		
UpdateRuleGroup	Otorga permiso para insertar o eliminar ActivatedRule objetos en un RuleGroup	Escritura	rulegroup*		
UpdateSizeConstraintSet	Otorga permiso para insertar o eliminar SizeConstraint objetos en un SizeConstraintSet	Escritura	sizeconstraintset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateSqlInjectionMatchSet	Otorga permiso para insertar o eliminar SqlInjectionMatchTuple objetos en un SqlInjectionMatchSet	Escritura	sqlinjectionmatchset*		
UpdateWebACL	Otorga permiso para insertar o eliminar ActivatedRule objetos en una WebACL	Administración de permisos	webacl*		
UpdateXssMatchSet	Otorga permiso para insertar o eliminar XssMatchTuple objetos en una XssMatchSet	Escritura	xssmatchset*		

Tipos de recursos definidos por AWS WAF Regional

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}`	

Tipos de recurso	ARN	Claves de condición
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
ratebasedrule	arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf-regional:${Region}:${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf-regional:${Region}:${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

Claves de condición para AWS WAF Regional

AWS WAF Regional define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función del conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función del valor-etiqueta asociado con el recurso.	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de etiquetas obligatorias en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición para AWS WAF V2

AWS El WAF V2 (prefijo de servicio:`wafv2`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS WAF V2

- Tipos de recursos definidos por AWS WAF V2
- Claves de condición para AWS WAF V2

Acciones definidas por AWS WAF V2

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Associate WebACL	Concede permiso para asociar una WebACL a un recurso	Write	webacl*		amplify:AssociateWebACL apigateway:SetWebACL apprunner:AssociateWebAcl appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl elasticloadbalanci

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					ng:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CheckCapacity	Concede permiso para calcular los requisitos de la unidad de capacidad de ACL web (WCU) para un ámbito y un conjunto de reglas especificados	Lectura			
CreateAPIKey	Otorga permiso para crear una clave de API para utilizarla en la integración de la API de CAPTCHA en las aplicaciones de sus clientes JavaScript	Escritura			
CreateIPSet	Otorga permiso para crear una IPSet	Escritura	ipset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexPatternSet	Otorga permiso para crear un RegexPatternSet	Escritura	regexpatternset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateRuleGroup	Otorga permiso para crear un RuleGroup	Escritura	rulegroup*		wafv2:TagResource
			ipset		
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	Concede permiso para crear una WebACL	Escritura	webacl*		wafv2:TagResource
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAPIKey	Otorga permiso para eliminar una clave API	Escritura			
DeleteFirewallManagerRuleGroups	Otorga permiso para eliminar FirewallManagedRulesGroups contenido de una WebACL si el Firewall Manager ya no lo gestiona	Escritura	webacl*		
DeleteIPSet	Otorga permiso para eliminar un IPSet	Escritura	ipset*		
DeleteLoggingConfiguration	Otorga permiso para eliminarlos LoggingConfiguration de una WebACL	Escritura	webacl*		
				wafv2:LogScope	
DeletePermissionPolicy	Otorga permiso para eliminarlo PermissionPolicy en un RuleGroup	Administración de permisos	rulegroup*		
DeleteRegexPatternSet	Otorga permiso para eliminar un RegexPatternSet	Escritura	regexpatternset*		
DeleteRuleGroup	Otorga permiso para eliminar un RuleGroup	Escritura	rulegroup*		
DeleteWebACL	Concede permiso para eliminar una WebACL	Escritura	webacl*		
DescribeAllManagedProducts	Concede permiso para recuperar información de producto para un grupo de reglas administrado	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeManagedProductsByVendor	Concede permiso para recuperar información de producto para un grupo de reglas administrado por un proveedor determinado	Lectura			
DescribeManagedRuleGroup	Concede permiso para recuperar información de alto nivel para un grupo de reglas administrado	Lectura			
DisassociateFirewallManager [solo permiso]	Concede permiso para desasociar Firewall Manager de una WebACL	Escritura	webacl*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateWebACL	Concede permiso para desasociar una WebACL de un recurso de aplicación	Escritura	amplify-app		amplify:DisassociateWebACL apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					wafv2:PutPermissionPolicy
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
GenerateMobileSdkReleaseUrl	Concede permiso para generar una URL de descarga prefirmada para la versión especificada del SDK móvil	Lectura			
GetDecryptedAPIKey	Concede permiso para devolver la clave de API de manera descifrada Utilice esta opción para comprobar los dominios de token que ha definido para la clave	Lectura			
GetIPSet	Otorga permiso para recuperar detalles sobre un IPSet	Lectura	ipset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetLoggingConfiguration	Otorga permiso de recuperación LoggingConfiguration para una WebACL	Lectura	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	Otorga permiso para recuperar detalles sobre un ManagedRuleSet	Lectura	managedruleset*		
GetMobileSdkRelease	Concede permiso para recuperar información de la versión del SDK móvil especificada, incluidas las notas y etiquetas de la versión	Lectura			
GetPermissionPolicy	Otorga permiso para recuperar un PermissionPolicy para un RuleGroup	Lectura	rulegroup*		
GetRateBasedStatementManagedKeys	Concede permiso para recuperar las claves que actualmente están bloqueadas por una regla basada en frecuencia	Lectura	webacl*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRegexPatternSet	Otorga permiso para recuperar detalles sobre un RegexPatternSet	Lectura	regexpatternset*		
				aws:ResourceTag/${TagKey}	
GetRuleGroup	Otorga permiso para recuperar detalles sobre un RuleGroup	Lectura	rulegroup*		
				aws:ResourceTag/${TagKey}	
GetSampledRequests	Concede permiso para recuperar información detallada sobre un muestreo de solicitudes web	Read	webacl*		
GetWebACL	Concede permiso para recuperar los detalles de una WebACL	Read	webacl*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetWebACLForResource	Concede permiso para recuperar la WebACL asociada a un recurso	Lectura	webacl*		amplify:GetWebACLForResource apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL
			amplify-app		
			apigateway		
			apprunner		
			appsync		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			loadbalancer/app/		
			userpool		
			verified-access-instance		
ListAPIKeys	Concede permiso para recuperar una lista de las claves de API que ha definido para el ámbito especificado	Enumeración			
ListAvailableManagedRuleGroupVersions	Concede permiso para recuperar una matriz de versiones de grupos de reglas administrados que están disponibles para su uso	Enumeración			
ListAvailableManagedRuleGroups	Concede permiso para recuperar una matriz de grupos de reglas administrados que están disponibles para su uso	Enumeración			
ListIPSets	Otorga permiso para recuperar una matriz de objetos de IPSet resumen para los conjuntos de IP que administra	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLoggingConfigurations	Otorga permiso para recuperar una matriz de sus LoggingConfiguration objetos	Enumeración		wafv2:LogScope	
ListManagedRuleSets	Otorga permiso para recuperar una matriz de tus ManagedRuleSet objetos	Enumeración			
ListMobileSdkReleases	Concede permiso para recuperar una lista de las versiones disponibles para el SDK móvil y la plataforma de dispositivos especificada	Enumeración			
ListRegexPatternSets	Otorga permiso para recuperar una matriz de RegexPatternSetSummary objetos para los conjuntos de patrones de expresiones regulares que gestione	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourcesForWebACL	Otorga permiso para recuperar una matriz de los nombres de recursos de Amazon (ARNs) para los recursos que están asociados a una ACL web	Enumeración	webacl*		amplify:ListResourcesForWebACL apprunner:ListAssociatedServicesForWebAcl cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations
			amplify-app		
			apprunner		
			userpool		
			verified-access-instance		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListRuleGroups	Otorga permiso para recuperar una matriz de RuleGroupSummary objetos para los grupos de reglas que administra	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	
ListWebACLs	Otorga permiso para recuperar una matriz de ACLSummary objetos web para la web ACLs que usted administra	Enumeración			
PutFirewallManagerRuleGroups [solo permiso]	Otorga permiso para crear FirewallManagedRulesGroups en una WebACL	Escritura	webacl*		
PutLoggingConfiguration	Otorga permiso para habilitar una LoggingConfiguration ACL web y empezar a registrarla	Escritura	webacl*		iam:CreateServiceLinkedRole

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	Otorga permiso para permitir la creación de una versión nueva o la actualización de una versión existente ManagedRuleSet	Escritura	managedruleset*		
			rulegroup*		
PutPermissionPolicy	Concede permiso para adjuntar una política de IAM a un recurso, que se utiliza para compartir grupos de reglas entre cuentas	Administración de permisos	rulegroup*		
TagResource	Otorga permiso para asociar etiquetas a un AWS recurso	Etiquetado	ipset		
			regexpatternset		
			rulegroup		
			webacl		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Otorga permiso para desasociar etiquetas de un recurso AWS	Etiquetado	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateIPSet	Otorga permiso para actualizar un IPSet	Escritura	ipset*		
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	Otorga permiso para actualizar la fecha de caducidad de una versión en ManagedRuleSet	Escritura	managedruleset*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRegexPatternSet	Otorga permiso para actualizar un RegexPatternSet	Escritura	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	Otorga permiso para actualizar un RuleGroup	Escritura	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	
UpdateWebACL	Concede permiso para actualizar una WebACL	Escritura	webacl*		
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS WAF V2

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}`	aws:ResourceTag/${TagKey}
managedruleset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/managedruleset/${Name}/${Id}`	
rulegroup	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}`	aws:ResourceTag/${TagKey}
regexpatternset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}`	aws:ResourceTag/${TagKey}
loadbalancer/app/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	

Tipos de recurso	ARN	Claves de condición
apigateway	`arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/${StageName}`	
appsync	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}`	
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	
apprunner	`arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}`	
verified-access-instance	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`	
amplify-app	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}`	

Claves de condición para AWS WAF V2

AWS El WAF V2 define las siguientes claves de condición que se pueden utilizar como `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por el conjunto de valores permitidos para cada una de las etiquetas.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso según el valor-etiqueta asociado con el recurso	Cadena
aws:TagKeys	Filtra el acceso por la presencia de etiquetas obligatorias en la solicitud	ArrayOfString
wafv2:LogDestinationResource	Filtra el acceso por ARN de destino del registro para la API PutLoggingConfiguration	ARN
wafv2:LogScope	Filtra el acceso por el ámbito de registro para la API de configuración de registro	Cadena

Acciones, recursos y claves de condición para AWS Well-Architected Tool

AWS Well-Architected Tool (prefijo de servicio`wellarchitected`:) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Well-Architected Tool
- Tipos de recursos definidos por AWS Well-Architected Tool

- Claves de condición para AWS Well-Architected Tool

Acciones definidas por AWS Well-Architected Tool

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna de nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la

columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateLenses	Concede el permiso para asociar una lente a la carga de trabajo especificada.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
AssociateProfiles	Concede permiso para asociar un perfil a la carga de trabajo especificada	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
ConfigureIntegration [solo permiso]	Concede permiso para configurar la integración	Escritura			
CreateLensShare	Otorga permiso al propietario de una lente para compartir la con otras AWS cuentas y usuarios de IAM	Escritura	lens*		
				aws:ResourceTag/${TagKey}	
CreateLensVersion	Concede permiso para crear una nueva versión de lente.	Escritura	lens*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
CreateMilestone	Concede el permiso para crear un nuevo hito para la carga de trabajo especificada.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
CreateProfile	Concede permiso para crear un nuevo proyecto	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileShare	Otorga permiso al propietario de un perfil para compartirlo con otras AWS cuentas y usuarios de IAM	Escritura	profile*		
				aws:ResourceTag/${TagKey}	
CreateReviewTemplate	Concede permiso para crear una nueva plantilla de revisión	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTemplateShare	Otorga permiso al propietario de una plantilla de revisión para compartirla con otras AWS cuentas y usuarios de IAM	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	
CreateWorkload	Concede el permiso para crear una nueva carga de trabajo.	Write		aws:RequestTag/${TagKey} aws:TagKeys wellarchitected:JiraProjectKey	
CreateWorkloadShare	Concede el permiso para compartir una carga de trabajo con otra cuenta.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
DeleteLens	Concede permiso para eliminar una lente.	Escritura	lens*		
				aws:ResourceTag/${TagKey}	
DeleteLensShare	Concede permiso para eliminar una cuota de carga de trabajo existente.	Escritura	lens*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeleteProfile	Concede permiso para eliminar un perfil	Escritura	profile*		
				aws:ResourceTag/${TagKey}	
DeleteProfileShare	Concede permiso para eliminar un recurso compartido o de perfil existente	Escritura	profile*		
				aws:ResourceTag/${TagKey}	
DeleteReviewTemplate	Concede permiso para eliminar una plantilla de revisión existente	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteTemplateShare	Concede permiso para eliminar un uso compartido de plantilla de revisión existente	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteWorkload	Concede el permiso para eliminar una carga de trabajo existente.	Write	workload*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
DeleteWorkloadShare	Concede el permiso para eliminar una cuota de carga de trabajo existente.	Write	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateLenses	Concede el permiso para desasociar una lente de la carga de trabajo especificada.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateProfiles	Concede permiso para desasociar un perfil de la carga de trabajo especificada	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
ExportLens	Concede permiso para exportar una lente existente	Lectura	lens*		
				aws:ResourceTag/${TagKey}	
GetAnswer	Concede el permiso para recuperar la respuesta especificada de la revisión de lente especificada.	Lectura	workload*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetConsolidatedReport	Concede permiso para obtener las métricas del informe consolidado o para generar un PDF del informe consolidado en esta cuenta	Lectura			
GetGlobalSettings	Concede permiso para obtener todas las configuraciones de la cuenta	Lectura			
GetLens	Concede permiso para obtener una lente existente.	Lectura	lens*		
				aws:ResourceTag/${TagKey}	
GetLensReview	Concede el permiso para recuperar la revisión de lente especificada de la carga de trabajo especificada.	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetLensReviewReport	Concede el permiso para recuperar el informe para la revisión de lente especificada.	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetLensVersionDifference	Concede el permiso para obtener la diferencia entre la versión de lente especificada y la última versión de lente disponible.	Read	lens*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMilestone	Concede permiso para recuperar el hito especificado de la carga de trabajo especificada	Lectura	workload*		
				aws:ResourceTag/${TagKey}	
GetProfile	Concede permiso para recuperar el perfil especificado	Lectura	profile*		
				aws:ResourceTag/${TagKey}	
GetProfileTemplate	Concede permiso para recuperar la plantilla de perfil especificada	Lectura			
GetReviewTemplate	Concede permiso para recuperar la plantilla de revisión especificada	Lectura	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateAnswer	Concede el permiso para recuperar la respuesta especificada de la revisión de lente de plantilla especificada.	Lectura	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateLensReview	Concede el permiso para recuperar la revisión de lente especificada de la plantilla de revisión especificada.	Lectura	review-template*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
GetWorkload	Concede el permiso para recuperar la carga de trabajo especificada.	Lectura	workload*		
				aws:ResourceTag/${TagKey}	
ImportLens	Concede permiso para importar una nueva lente.	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
ListAnswers	Concede el permiso para enumerar las respuestas de la revisión de lente especificada.	Enumeración	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckDetails	Concede permiso para enumerar los detalles de comprobación de la carga de trabajo	Enumeración	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckSummaries	Concede permiso para enumerar los resúmenes de comprobación de la carga de trabajo	Enumeración	workload*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListLensReviewImprovements	Concede el permiso para enumerar las mejoras de la revisión de lente especificada.	List	workload*		
				aws:ResourceTag/${TagKey}	
ListLensReviews	Concede el permiso para enumerar las revisiones de lente de la carga de trabajo especificada.	Enumeración	workload*		
				aws:ResourceTag/${TagKey}	
ListLensShares	Concede permiso para enumerar todos los recursos compartidos creados para un objetivo	Enumeración	lens*		
				aws:ResourceTag/${TagKey}	
ListLenses	Concede el permiso para enumerar las lentes disponibles para esta cuenta.	List			
ListMilestones	Concede el permiso para enumerar los hitos de la carga de trabajo especificada.	List	workload*		
				aws:ResourceTag/${TagKey}	
ListNotifications	Concede el permiso para enumerar las notificaciones relacionadas con la cuenta o el recurso especificado.	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListProfileNotifications	Concede permiso para enumerar las notificaciones de perfil relacionadas con el recurso especificado	Enumeración			
ListProfileShares	Concede permiso para enumerar todos los recursos compartidos creados para un perfil	Enumeración	profile*		
				aws:ResourceTag/${TagKey}	
ListProfiles	Concede permiso para enumerar los perfiles disponibles para esta cuenta	Enumeración			
ListReviewTemplateAnswers	Concede permiso para enumerar las respuestas de la plantilla de revisión de lente especificada.	Enumeración	review-template*		
				aws:ResourceTag/${TagKey}	
ListReviewTemplates	Concede permiso para enumerar las plantillas de revisión disponibles para esta cuenta.	Enumeración			
ListShareInvitations	Concede el permiso para enumerar las invitaciones de cuota de carga de trabajo de la cuenta o usuario especificados.	List			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListTagsForResource	Concede permiso para enumerar las etiquetas para un recurso Well-Architected.	Lectura	lens		
			profile		
			review-template		
			workload		
				aws:ResourceTag/${TagKey}	
ListTemplateShares	Concede permiso para enumerar todos los usos compartidos creados para una plantilla de revisión	Enumeración	review-template*		
				aws:ResourceTag/${TagKey}	
ListWorkloadShares	Concede el permiso para enumerar las cuotas de carga de trabajo de la carga de trabajo especificada.	List	workload*		
				aws:ResourceTag/${TagKey}	
ListWorkloads	Concede el permiso para enumerar las cargas de trabajo de esta cuenta.	List			
TagResource	Concede permiso para etiquetar un recurso Well-Architected.	Etiquetado	lens		
			profile		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			review-template		
			workload		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar la etiqueta de un recurso Well-Architected.	Etiquetado	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys	
UpdateAnswer	Concede el permiso para actualizar las propiedades de la respuesta especificada.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
UpdateGlobalSettings	Concede permiso para administrar todas las configuraciones para la cuenta	Escritura		wellarchitected:JiraProjectKey	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIntegration	Concede permiso para actualizar las propiedades de la integración	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
UpdateLensReview	Concede el permiso para actualizar las propiedades de la revisión de lente especificada.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
UpdateProfile	Concede permiso para actualizar las propiedades del perfil especificado	Escritura	profile*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplate	Concede permiso para actualizar las propiedades de la plantilla de revisión especificada.	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateAnswer	Concede permiso para actualizar las propiedades de la respuesta de la plantilla de revisión especificada.	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateReviewTemplateLensReview	Concede permiso para actualizar las propiedades de la revisión de lente de plantilla de revisión especificada.	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateShareInvitation	Concede el permiso para actualizar el estado de la invitación de la cuota de la carga de trabajo especificada.	Write			
UpdateWorkload	Concede el permiso para actualizar las propiedades de la carga de trabajo especificada.	Escritura	workload*		
				aws:ResourceTag/${TagKey} wellarchitected:JiraProjectKey	
UpdateWorkloadShare	Concede permiso para actualizar las propiedades de la carga de trabajo compartida especificada	Escritura	workload*		
				aws:ResourceTag/${TagKey}	
UpgradeLensReview	Concede el permiso para actualizar la revisión de lente especificada para utilizar la última versión del objetivo asociado.	Escritura	workload*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpgradeProfileVersion	Concede permiso para actualizar la carga de trabajo especificada para que utilice la versión más reciente del perfil asociado	Escritura	profile*		
			workload*		
				aws:ResourceTag/${TagKey}	
UpgradeReviewTemplateLensReview	Concede permiso para actualizar la revisión de lente especificada de la carga de trabajo especificada.	Escritura	review-template*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por AWS Well-Architected Tool

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
workload	`arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
lens	`arn:${Partition}:wellarchitected:${Region}:${Account}:lens/${ResourceId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:wellarchitected:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
review-template	`arn:${Partition}:wellarchitected:${Region}:${Account}:review-template/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Well-Architected Tool

AWS Well-Architected Tool define las siguientes claves de condición que se pueden utilizar en `Condition` el elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta de la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra los accesos mediante las claves de etiqueta en la solicitud	ArrayOfString

Claves de condición	Descripción	Tipo
wellarchitected:JiraProjectKey	Filtra el acceso por clave de proyecto	Cadena

Acciones, recursos y claves de condición para AWS Wickr

AWS Wickr (prefijo de servicio:`wickr`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS Wickr
- Tipos de recursos definidos por AWS Wickr
- Claves de condición para AWS Wickr

Acciones definidas por AWS Wickr

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

En la columna Nivel de acceso de la tabla Acciones se describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de

acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateAdminSession	Otorga permiso para crear y gestionar redes de Wickr	Escritura	network*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateNetwork	Concede permiso para crear una nueva red de Wickr	Escritura			
DeleteNetwork	Concede permiso para crear y eliminar redes de Wickr	Escritura			
ListNetworks	Otorga permiso para ver las redes de Wickr	Escritura			
ListTagsForResource	Concede permiso para enumerar las etiquetas aplicadas a un recurso de Wickr	Lectura			
TagResource	Concede permiso para agregar etiquetas a un recurso de Wickr especificado	Etiquetado	network*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para quitar las etiquetas especificadas del recurso de Wickr especificado	Etiquetado	network*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateNetworkDetails	Concede permiso para actualizar los detalles de red de Wickr	Escritura	network*		

Tipos de recursos definidos por AWS Wickr

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
network	`arn:${Partition}:wickr:${Region}:${Account}:network/${NetworkId}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS Wickr

AWS Wickr define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por la clave y el valor de una etiqueta en una solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiqueta en una solicitud	ArrayOfString

Acciones, recursos y claves de condición de Amazon WorkDocs

Amazon WorkDocs (prefijo de servicio:`workdocs`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkDocs
- Tipos de recursos definidos por Amazon WorkDocs
- Claves de estado de Amazon WorkDocs

Acciones definidas por Amazon WorkDocs

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o

comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AbortDocumentVersionUpload	Otorga permiso para abortar la carga de la versión del documento especificada iniciada previamente por InitiateDocumentVersionUpload	Escritura			
ActivateUser	Concede permiso para activar el usuario especificado. Solo los usuarios activos pueden acceder a Amazon WorkDocs	Escritura			
AddNotificationPermissions [solo permiso]	Otorga permiso para añadir a los directores que pueden llamar a la suscripción a notificaciones APIs de un sitio determinado WorkDocs	Escritura			
AddResourcePermissions	Concede permiso para crear un conjunto de permisos para la carpeta o documento especificados	Escritura			
AddUserToGroup [solo permiso]	Concede permiso para agregar un usuario a un grupo	Escritura			
CheckAlias [solo permiso]	Concede permiso para comprobar un alias	Lectura			
CreateComment	Concede permiso para agregar un nuevo comentari	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	o a la versión del documento especificada				
CreateCustomMetadata	Concede permiso para agregar una o varias propiedades personalizadas al recurso especificado	Escritura			
CreateFolder	Concede permiso para crear una carpeta con la carpeta principal y el nombre especificados	Escritura			
CreateInstance [solo permiso]	Concede permiso para crear una instancia	Escritura			
CreateLabels	Concede permiso para agregar etiquetas al recurso determinado	Escritura			
CreateNotificationSubscription	Otorga permiso WorkDocs para configurar el uso de las notificaciones de Amazon SNS	Escritura			
CreateUser	Concede permiso para crear un usuario en un directorio de Microsoft AD o Simple AD	Escritura			
DeactivateUser	Otorga permiso para desactivar al usuario especificado, lo que revoca el acceso del usuario a Amazon WorkDocs	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteComment	Concede permiso para eliminar el comentario especificado de la versión del documento	Escritura			
DeleteCustomMetadata	Concede permiso para eliminar metadatos personalizados del recurso especificado	Escritura			
DeleteDocument	Concede permiso para eliminar permanentemente el documento especificado y sus metadatos asociados	Escritura			
DeleteDocumentVersion	Otorga permiso para eliminar versiones de un documento especificado	Escritura			
DeleteFolder	Concede permiso para eliminar permanentemente la carpeta especificada y su contenido	Escritura			
DeleteFolderContents	Concede permiso para eliminar el contenido de la carpeta especificada	Escritura			
DeleteInstance [solo permiso]	Concede permiso para eliminar una instancia	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteLabels	Concede permiso para eliminar una o varias etiquetas de un recurso	Escritura			
DeleteNotification Permissions [solo permiso]	Otorga permiso para eliminar a los directores que pueden llamar a la suscripción a notificaciones de un sitio APIs determinado WorkDocs	Escritura			
DeleteNotification Subscription	Concede permiso para eliminar la suscripción especificada de la organización especificada	Escritura			
DeleteUser	Concede permiso para eliminar el usuario especificado de un directorio de Microsoft AD o Simple AD	Escritura			
DeregisterDirectory [solo permiso]	Concede permiso para anular el registro de un directorio	Escritura			
DescribeActivities	Concede permiso para recuperar las actividades del usuario en un periodo de tiempo especificado	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAvailableDirectories [solo permiso]	Concede permiso para describir los directorios disponibles	Enumeración			
DescribeComments	Concede permiso para obtener una lista de todos los comentarios de la versión del documento especificada	Enumeración			
DescribeDocumentVersions	Concede permiso para recuperar las versiones del documento para el documento especificado	Enumeración			
DescribeFolderContents	Concede permiso para describir el contenido de la carpeta especificada, incluidos sus documentos y subcarpetas	Enumeración			
DescribeGroups	Concede permiso para describir los grupos de usuarios	Enumeración			
DescribeInstanceExports [solo permiso]	Concede permiso para describir el historial de exportación para una instancia	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeInstances [solo permiso]	Concede permiso para describir instancias	Enumeración			
DescribeNotificationPermissions [solo permiso]	Otorga permiso para describir a los directores que pueden llamar a la suscripción a notificaciones en un APIs sitio determinado WorkDocs	Enumeración			
DescribeNotificationSubscriptions	Concede permiso para obtener una lista de las suscripciones a notificaciones especificadas	Enumeración			
DescribeResourcePermissions	Concede permiso para ver una descripción de los permisos de un recurso especificado	Enumeración			
DescribeRootFolders	Concede permiso para describir las carpetas raíz	Enumeración			
DescribeUsers	Concede permiso para ver una descripción de los usuarios especificados. Se pueden describir todos los usuarios o filtrar los resultados (por ejemplo, por estado u organización)	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DownloadDocumentVersion [solo permiso]	Concede permiso para descargar una versión del documento especificada	Lectura			
GetCurrentUser	Concede permiso para recuperar los detalles del usuario actual	Lectura			
GetDocument	Concede permiso para recuperar el objeto de documento especificado	Lectura			
GetDocumentPath	Concede permiso para recuperar la información de ruta (la jerarquía de la carpeta raíz) del documento solicitado	Lectura			
GetDocumentVersion	Concede permiso para recuperar los metadatos de la versión para el documento especificado	Lectura			
GetFolder	Concede permiso para recuperar los metadatos de la carpeta especificada	Lectura			
GetFolderPath	Concede permiso para recuperar la información de ruta (la jerarquía de la carpeta raíz) de la carpeta especificada	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetGroup [solo permiso]	Concede permiso para recuperar detalles del grupo especificado	Lectura			
GetResources	Concede permiso para obtener una colección de recursos	Lectura			
InitiateDocumentVersionUpload	Concede permiso para crear un nuevo objeto de documento y objeto de versión	Escritura			
RegisterDirectory [solo permiso]	Concede permiso para registrar un directorio	Escritura			
RemoveAllResourcePermissions	Concede permiso para eliminar todos los permisos del recurso especificado	Escritura			
RemoveResourcePermission	Concede permiso para eliminar el permiso de la entidad principal especificada del recurso especificado	Escritura			
RestoreDocumentVersions	Otorga permiso para restaurar versiones de un documento especificado	Escritura			
SearchResources	Concede permiso para buscar en los metadatos y el contenido de los recursos	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
StartInstanceExport [solo permiso]	Concede permiso para iniciar una exportación para una instancia	Escritura	organization*		
UpdateDocument	Concede permiso para actualizar los atributos especificados del documento especificado	Escritura			
UpdateDocumentVersion	Concede permiso para cambiar el estado de la versión del documento a ACTIVE (ACTIVO)	Escritura			
UpdateFolder	Concede permiso para actualizar los atributos especificados de la carpeta especificada	Escritura			
UpdateInstanceAlias [solo permiso]	Concede permiso para actualizar un alias de instancia	Escritura			
UpdateUser	Otorga permiso para actualizar los atributos especificados del usuario especificado y concede o revoca los privilegios administrativos del sitio de Amazon WorkDocs	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateUserAdministrativeSettings [solo permiso]	Concede permiso para actualizar la configuración administrativa de un usuario	Escritura			

Tipos de recursos definidos por Amazon WorkDocs

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
organization	`arn:${Partition}:workdocs:${Region}:${Account}:organization/${ResourceId}`	

Claves de estado de Amazon WorkDocs

WorkDocs no tiene claves de contexto específicas de un servicio que puedan usarse en el `Condition` elemento de las declaraciones de políticas. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de Amazon WorkLink

Amazon WorkLink (prefijo de servicio:`worklink`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkLink
- Tipos de recursos definidos por Amazon WorkLink
- Claves de estado de Amazon WorkLink

Acciones definidas por Amazon WorkLink

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateDomain	Otorga permiso para asociar un dominio a una WorkLink flota de Amazon	Escritura	fleet*		
AssociateWebsiteAuthorizationProvider	Otorga permiso para asociar un proveedor de autorización de sitios web con una WorkLink flota de Amazon	Escritura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateWebsiteCertificateAuthority	Otorga permiso para asociar una autoridad de certificación de sitios web con una WorkLink flota de Amazon	Escritura	fleet*		
CreateFleet	Otorga permiso para crear una WorkLink flota de Amazon	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFleet	Otorga permiso para eliminar una WorkLink flota de Amazon	Escritura	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAuditStreamConfiguration	Otorga permiso para describir la configuración del flujo de auditoría de una WorkLink flota de Amazon	Lectura	fleet*		
DescribeCompanyNetworkConfiguration	Otorga permiso para describir la configuración de red de la empresa para una WorkLink flota de Amazon	Lectura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeDevice	Otorga permiso para describir los detalles de un dispositivo asociado a una WorkLink flota de Amazon	Lectura	fleet*		
DescribeDevicePolicyConfiguration	Otorga permiso para describir la configuración de la política de dispositivos para una WorkLink flota de Amazon	Lectura	fleet*		
DescribeDomain	Otorga permiso para describir detalles sobre un dominio asociado a una WorkLink flota de Amazon	Lectura	fleet*		
DescribeFleetMetadata	Otorga permiso para describir los metadatos de una WorkLink flota de Amazon	Lectura	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIdentityProviderConfiguration	Otorga permiso para describir la configuración del proveedor de identidad para una WorkLink flota de Amazon	Lectura	fleet*		
DescribeWebsiteCertificateAuthority	Otorga permiso para describir un sitio web (autoridad de certificación) asociada a una WorkLink flota de Amazon	Lectura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateDomain	Otorga permiso para desasociar un dominio de una flota de Amazon WorkLink	Escritura	fleet*		
DisassociateWebsiteAuthorizationProvider	Otorga permiso para desvincular a un proveedor de autorización de sitios web de una flota de Amazon WorkLink	Escritura	fleet*		
DisassociateWebsiteCertificateAuthority	Otorga permiso para desasociar una autoridad de certificación de un sitio web de una flota de Amazon WorkLink	Escritura	fleet*		
ListDevices	Otorga permiso para publicar los dispositivos asociados a una WorkLink flota de Amazon	Enumeración	fleet*		
ListDomains	Otorga permiso para enumerar los dominios asociados a una WorkLink flota de Amazon	Enumeración	fleet*		
ListFleets	Otorga permiso para publicar las WorkLink flotas de Amazon asociadas a la cuenta	Enumeración			
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListWebsiteAuthorizationProviders	Otorga permiso para incluir los proveedores de autorización del sitio web para una WorkLink flota de Amazon	Enumeración	fleet*		
ListWebsiteCertificateAuthorities	Otorga permiso para incluir las autoridades de certificación del sitio web asociadas a una WorkLink flota de Amazon	Enumeración	fleet*		
RestoreDomainAccess	Otorga permiso para restablecer el acceso a un dominio asociado a una WorkLink flota de Amazon	Escritura	fleet*		
RevokeDomainAccess	Otorga permiso para revocar el acceso a un dominio asociado a una flota de Amazon WorkLink	Escritura	fleet*		
SearchEntity [solo permiso]	Otorga permiso para publicar dispositivos para una WorkLink flota de Amazon	Enumeración	fleet*		
SignOutUser	Otorga permiso para cerrar la sesión de un usuario de una WorkLink flota de Amazon	Escritura	fleet*		
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso.	Etiquetado	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	fleet*		
				aws:TagKeys	
UpdateAuditStreamConfiguration	Otorga permiso para actualizar la configuración del flujo de auditoría de una WorkLink flota de Amazon	Escritura	fleet*		
UpdateCompanyNetworkConfiguration	Otorga permiso para actualizar la configuración de red de la empresa para una WorkLink flota de Amazon	Escritura	fleet*		
UpdateDevicePolicyConfiguration	Otorga permiso para actualizar la configuración de la política de dispositivos para una WorkLink flota de Amazon	Escritura	fleet*		
UpdateDomainMetadata	Otorga permiso para actualizar los metadatos de un dominio asociado a una WorkLink flota de Amazon	Escritura	fleet*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateFleetMetadata	Otorga permiso para actualizar los metadatos de una WorkLink flota de Amazon	Escritura	fleet*		
UpdateIdentityProviderConfiguration	Otorga permiso para actualizar la configuración del proveedor de identidad de una WorkLink flota de Amazon	Escritura	fleet*		

Tipos de recursos definidos por Amazon WorkLink

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
fleet	`arn:${Partition}:worklink::${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon WorkLink

Amazon WorkLink define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones en función de la presencia de pares de clave-valor de etiqueta en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de pares de clave-valor de etiqueta adjuntados al recurso	Cadena
aws:TagKeys	Filtra acciones en función de la presencia de claves de etiqueta en la solicitud.	ArrayOfString

Acciones, recursos y claves de condición de Amazon WorkMail

Amazon WorkMail (prefijo de servicio:`workmail`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkMail
- Tipos de recursos definidos por Amazon WorkMail
- Claves de estado de Amazon WorkMail

Acciones definidas por Amazon WorkMail

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AllowVendedLogDeliveryForResource [solo permiso]	Otorga permiso para configurar la entrega de registros vendidos para los registros de auditoría WorkMail	Escritura	organization*		
AssociateDelegateToResource	Concede permiso para agregar a un miembro (usuario o grupo) al conjunto de delegados del recurso	Write	organization*		
AssociateMemberToGroup	Concede permiso para agregar un miembro (usuario o grupo) al conjunto del grupo	Escritura	organization*		
AssumeImpersonationRole	Otorga permiso para asumir una función de suplantación de identidad para la organización de Amazon en cuestión WorkMail	Escritura	organization*		
CancelMailboxExportJob	Concede permiso para cancelar un trabajo de exportación de bandeja de entrada actualmente en ejecución	Escritura	organization*		
CreateAlias	Otorga permiso para añadir un alias al conjunto de un	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	miembro (usuario o grupo) determinado de WorkMail				
CreateAvailabilityConfiguration	Otorga permiso para crear una AvailabilityConfiguration para la WorkMail organización y el dominio de Amazon en cuestión	Escritura	organization*		
CreateGroup	Otorga permiso para crear un grupo que se puede utilizar WorkMail mediante una llamada a la RegisterToWorkMail operación	Escritura	organization*		
CreateIdentityCenterApplication	Otorga permiso para crear una aplicación de Identity Center para WorkMail	Escritura			
CreateImpersonationRole	Otorga permiso para crear un rol de suplantación de identidad para la organización de Amazon en cuestión WorkMail	Escritura	organization*		
CreateInboundMailFlowRule [solo permiso]	Concede permiso para crear una regla de flujo de email entrante que se aplicará a todos los emails enviados a una organización	Write	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateMailDomain [solo permiso]	Concede permiso para crear un dominio de correo	Escritura	organization*		
CreateMobileDeviceAccessRule	Concede permiso para crear una nueva regla de acceso de dispositivos móviles	Escritura	organization*		
CreateOrganization	Otorga permiso para crear una nueva WorkMail organización de Amazon	Escritura			
CreateOutboundMailFlowRule [solo permiso]	Concede permiso para crear una regla de flujo de email saliente que se aplicará a todos los emails enviados desde una organización	Escritura	organization*		
CreateResource	Otorga permiso para crear un nuevo WorkMail recurso	Escritura	organization*		
CreateSmtpGateway [solo permiso]	Otorga permiso para registrar una puerta de enlace SMTP a una organización WorkMail	Escritura	organization*		
CreateUser	Otorga permiso para crear un usuario, que se puede activar posteriormente mediante una llamada a la operación RegisterToWorkMail	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteAccessControlRule	Concede permiso para eliminar una regla de control de acceso	Write	organization*		
DeleteAlias	Concede permiso para eliminar uno o varios alias especificados de un conjunto de alias de un usuario determinado	Escritura	organization*		
DeleteAvailabilityConfiguration	Otorga permiso AvailabilityConfiguration para eliminar la WorkMail organización y el dominio de Amazon en cuestión	Escritura	organization*		
DeleteEmailMonitoringConfiguration	Concede permiso para eliminar la configuración de supervisión de correo electrónico de una organización	Escritura	organization*		
DeleteGroup	Otorga permiso para eliminar un grupo de WorkMail	Escritura	organization*		
DeleteIdentityCenterApplication	Otorga permiso para eliminar una aplicación del Centro de Identidad para WorkMail	Escritura			
DeleteIdentityProviderConfiguration	Otorga permiso para eliminar la configuración del proveedor de identidad de la organización	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteImpersonationRole	Otorga permiso para eliminar un rol de suplantación de identidad para la organización de Amazon en cuestión WorkMail	Escritura	organization*		
DeleteInboundMailFlowRule [solo permiso]	Concede permiso para eliminar una regla de flujo de email entrante de modo que ya no se aplique a los emails enviados a una organización	Write	organization*		
DeleteMailDomain [solo permiso]	Concede permiso para quitar un dominio de correo sin uso de una organización	Write	organization*		
DeleteMailboxPermissions	Concede permiso para eliminar los permisos concedidos a un miembro (usuario o grupo)	Write	organization*		
DeleteMobileDevice [solo permiso]	Concede permiso para eliminar un dispositivo móvil de un usuario	Escritura	organization*		
DeleteMobileDeviceAccessOverride	Concede permiso para eliminar una invalidación de acceso de dispositivo móvil.	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteMobileDeviceAccessRule	Concede permiso para eliminar una regla de acceso de dispositivo móvil	Escritura	organization*		
DeleteOrganization	Otorga permiso para eliminar una WorkMail organización de Amazon y todos AWS los recursos subyacentes gestionados por Amazon WorkMail como parte de la organización	Escritura	organization*		
DeleteOutboundMailFlowRule [solo permiso]	Concede permiso para eliminar una regla de flujo de correo saliente de modo que ya no se aplique a los emails enviados desde una organización	Escritura	organization*		
DeletePersonalAccessToken	Otorga permiso para eliminar un token de acceso personal	Escritura	organization*		
DeleteResource	Concede permiso para eliminar el recurso especificado	Write	organization*		
DeleteRetentionPolicy	Concede permiso para eliminar la política de retención basada en los identificadores de políticas y organizaciones proporcionados	Write	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteSmtpGateway [solo permiso]	Concede permiso para eliminar una gateway SMTP de una organización	Escritura	organization*		
DeleteUser	Otorga permiso para eliminar un usuario de los sistemas posteriores WorkMail y de todos los sistemas posteriores	Escritura	organization*		
DeliverToMailbox [solo permiso]	Otorga permiso para enviar correos electrónicos a una WorkMail organización mediante la MailManager DeliverToMailbox acción SES	Escritura	organization*		
DeregisterFromWorkMail	Otorga permiso para marcar un usuario, grupo o recurso como si ya no se utiliza en WorkMail	Escritura	organization*		
DeregisterMailDomain	Concede permiso para quitar del registro un dominio de correo sin uso de una organización.	Escritura	organization*		
DescribeEmailMonitoringConfiguration	Concede permiso para recuperar la configuración de supervisión de correo electrónico de una organización	Lectura	organization*		
DescribeEntity	Concede permiso para leer detalles de una entidad.	Lectura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeGroup	Concede permiso para leer los detalles de un grupo	Enumeración	organization*		
DescribeIdentityProviderConfiguration	Otorga permiso para leer la configuración del proveedor de identidad de la organización	Lectura	organization*		
DescribeInboundDmarcSettings	Concede permiso para leer la configuración de una política DMARC para una organización específica	Lectura	organization*		
DescribeInboundMailFlowRule [solo permiso]	Concede permiso para devolver los detalles de una regla de flujo de email entrante configurada para una organización	Read	organization*		
DescribeMailDomains [solo permiso]	Concede permiso para mostrar los detalles de todos los dominios de correo asociados a la organización	Enumeración	organization*		
DescribeMailboxExportJob	Concede permiso para recuperar detalles de un trabajo de exportación de bandeja de entrada	Read	organization*		
DescribeOrganization	Concede permiso para leer los detalles de una organización	List	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeOutboundMailFlowRule [solo permiso]	Concede permiso para leer los detalles de una regla de flujo de correo saliente configurada para una organización	Read	organization*		
DescribeResource	Concede permiso para leer los detalles de un recurso	List	organization*		
DescribeSmtpGateway [solo permiso]	Concede permiso para leer los detalles de una gateway SMTP registrada en una organización	Read	organization*		
DescribeUser	Concede permiso para leer detalles de un usuario	Enumeración	organization*		
DisassociateDelegateFromResource	Concede permiso para eliminar un miembro del conjunto de delegados del recurso	Write	organization*		
DisassociateMemberFromGroup	Concede permiso para eliminar a un miembro de un grupo	Write	organization*		
EnableMailDomain [solo permiso]	Concede permiso para habilitar un dominio de correo en la organización	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccessControlEffect	Otorga permiso para obtener los efectos de las reglas de control de acceso tal como se aplican a una IPv4 dirección, acción de protocolo de acceso o ID de usuario específicos	Lectura	organization*		
GetDefaultRetentionPolicy	Concede permiso para recuperar la política de retención asociada en un nivel organizativo	Lectura	organization*		
GetImpersonationRole	Otorga permiso para recuperar un rol de suplantación de identidad para la organización de Amazon en cuestión WorkMail	Lectura	organization*		
GetImpersonationRoleEffect	Concede permiso para obtener el efecto de las reglas asociadas a un rol de suplantación de un usuario específico	Lectura	organization*		
GetJournalingRules [solo permiso]	Concede permiso para leer las direcciones de email configuradas en diario y de reserva para el registro en diario de email	Lectura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMailDomain	Concede permiso para recuperar detalles de un dominio de correo determinado en una organización.	Lectura	organization*		
GetMailDomainDetails [solo permiso]	Concede permiso para obtener los detalles del dominio de correo	Lectura	organization*		
GetMailboxDetails	Concede permiso para leer los detalles de la bandeja de entrada del usuario	Read	organization*		
GetMobileDeviceAccessEffect	Concede permiso para simular el efecto de las reglas de acceso de dispositivos móviles para los atributos dados de un evento de acceso de ejemplo	Lectura	organization*		
GetMobileDeviceAccessOverride	Concede permiso para recuperar una anulación de acceso a un dispositivo móvil.	Lectura	organization*		
GetMobileDeviceDetails [solo permiso]	Concede permiso para obtener los detalles del dispositivo móvil	Read	organization*		
GetMobileDevicesForUser [solo permiso]	Concede permiso para obtener una lista de los dispositivos móviles asociados al usuario	Read	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetMobilePolicyDetails [solo permiso]	Concede permiso para obtener los detalles de la política de dispositivos móviles asociada a la organización	Lectura	organization*		
GetPersonalAccessTokenMetadata	Otorga permiso para leer los metadatos de un token de acceso personal	Lectura	organization*		
ListAccessControlRules	Concede permiso para enumerar las reglas de control de acceso	Lectura	organization*		
ListAliases	Concede permiso para enumerar los alias asociados a una entidad determinada	Enumeración	organization*		
ListAvailabilityConfigurations	Otorga permiso para publicar todos los AvailabilityConfiguration elementos de la WorkMail organización de Amazon en cuestión	Lectura	organization*		
ListGroupMembers	Concede permiso para leer una descripción general de los miembros de un grupo Los usuarios y grupos pueden ser miembros de un grupo	List	organization*		
ListGroups	Concede permiso para enumerar resúmenes de los grupos de la organización	Enumeración	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListGroupsForEntity	Concede permiso para enumerar los grupos a los que pertenece una entidad	Enumeración	organization*		
ListImpersonationRoles	Otorga permiso para enumerar las funciones de suplantación de identidad de la organización de Amazon en cuestión WorkMail	Enumeración	organization*		
ListInboundMailFlowRules [solo permiso]	Concede permiso para enumerar las reglas de flujo de correo entrante configuradas para una organización	Enumeración	organization*		
ListMailDomains	Concede permiso para enumerar los dominios de correo para una organización determinada.	Enumeración	organization*		
ListMailboxExportJobs	Concede permiso para enumerar trabajos de exportación de bandeja de entrada	List	organization*		
ListMailboxPermissions	Concede permiso para mostrar los permisos de la bandeja de entrada asociados a una bandeja de entrada de usuario, grupo o recurso	Enumeración	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListMobileDeviceAccessOverrides	Concede permiso para enumerar las invalidaciones de acceso de dispositivos móviles.	Lectura	organization*		
ListMobileDeviceAccessRules	Concede permiso para enumerar las reglas de acceso de dispositivos móviles	Lectura	organization*		
ListOrganizations	Concede permiso para enumerar las organizaciones no eliminadas	List			
ListOutboundMailFlowRules [solo permiso]	Concede permiso para enumerar las reglas de flujo de correo saliente configuradas para una organización	Enumeración	organization*		
ListPersonalAccessTokens	Otorga permiso para incluir los metadatos de los tokens de acceso personal	Enumeración	organization*		
ListResourceDelegates	Concede permiso para enumerar los delegados asociados a un recurso	List	organization*		
ListResources	Concede permiso para enumerar los recursos de la organización	List	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSmtpGateways [solo permiso]	Concede permiso para enumerar gateways SMTP registradas en la organización	Enumeración	organization*		
ListTagsForResource	Otorga permiso para enumerar las etiquetas aplicadas a un recurso de WorkMail la organización de Amazon	Enumeración	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListUsers	Concede permiso para enumerar los usuarios de la organización	List	organization*		
PutAccessControlRule	Concede permiso para agregar una nueva regla de control de acceso	Escritura	organization*		
PutEmailMonitoringConfiguration	Concede permiso para agregar o actualizar la configuración de supervisión de correo electrónico de una organización	Escritura	organization*		
PutIdentityProviderConfiguration	Otorga permiso para añadir o actualizar la configuración del proveedor de identidad de la organización	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutInboundDmarcSettings	Concede permiso para habilitar o desactivar una política DMARC para una organización determinada	Escritura	organization*		
PutMailboxPermissions	Concede permiso para establecer permisos para un usuario, grupo o recurso, mediante el reemplazo de los permisos existentes	Escritura	organization*		
PutMobileDeviceAccessOverride	Concede permiso para agregar o actualizar una invalidación de acceso de dispositivo móvil.	Escritura	organization*		
PutRetentionPolicy	Concede permiso para agregar o actualizar la política de retención	Escritura	organization*		
RegisterMailDomain	Concede permiso para registrar un nuevo dominio de correo en una organización.	Escritura	organization*		
RegisterToWorkMail	Concede permiso para registrar un usuario, grupo o recurso existente y deshabilitado para su uso mediante la asociación de una bandeja de entrada y capacidades de calendario	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ResetPassword	Concede permiso para permitir que el administrador restablezca la contraseña de un usuario	Write	organization*		
SearchMembers [solo permiso]	Concede permiso para realizar una búsqueda de prefijos a fin de buscar un usuario específico o en un grupo de correo	Read	organization*		
SetDefaultMailDomain [solo permiso]	Concede permiso para establecer el dominio de correo predeterminado para la organización	Write	organization*		
SetJournalingRules [solo permiso]	Concede permiso para establecer el registro en diario y las direcciones de email alternativas para el registro en diario de email	Write	organization*		
SetMobilePolicyDetails [solo permiso]	Concede permiso para establecer los detalles de una política de dispositivos móviles asociada a la organización	Write	organization*		
StartMailboxExportJob	Concede permiso para iniciar un nuevo trabajo de exportación de bandeja de entrada	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
TagResource	Otorga permiso para etiquetar el recurso de WorkMail la organización Amazon especificado	Etiquetado	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestAvailabilityConfiguration	Concede permiso para realizar una prueba en un proveedor de disponibilidad a fin de garantizar que se permite el acceso	Lectura	organization*		
TestInboundMailFlowRules [solo permiso]	Concede permiso para probar qué reglas de entrada se aplicarán a un email con un remitente y destinatario determinados	Write	organization*		
TestOutboundMailFlowRules [solo permiso]	Concede permiso para probar qué reglas de salida se aplicarán a un email con un remitente y destinatario determinados	Escritura	organization*		
UntagResource	Otorga permiso para desetiquetar el recurso de la WorkMail organización Amazon especificado	Etiquetado	organization*		
				aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateAvailabilityConfiguration	Otorga permiso AvailabilityConfiguration para actualizar un dominio y una WorkMail organización de Amazon existentes	Escritura	organization*		
UpdateDefaultMailDomain	Concede permiso para actualizar qué dominio es el dominio predeterminado de una organización.	Escritura	organization*		
UpdateGroup	Concede permiso para actualizar los detalles de un grupo	Escritura	organization*		
UpdateImpersonationRole	Otorga permiso para actualizar un rol de suplantación de identidad existente para la organización de Amazon en cuestión WorkMail	Escritura	organization*		
UpdateInboundMailFlowRule [solo permiso]	Concede permiso para actualizar los detalles de una regla de flujo de email entrante que se aplicará a todos los emails enviados a una organización	Write	organization*		
UpdateMailboxQuota	Concede permiso para actualizar el tamaño máximo (en MB) de la bandeja de entrada del usuario	Escritura	organization*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateMobileDeviceAccessRule	Concede permiso para actualizar una regla de acceso de dispositivo móvil.	Escritura	organization*		
UpdateOutboundMailFlowRule [solo permiso]	Concede permiso para actualizar los detalles de una regla de flujo de email saliente que se aplicará a todos los emails enviados desde una organización	Write	organization*		
UpdatePrimaryEmailAddress	Concede permiso para actualizar el email principal de un usuario, grupo o recurso	Write	organization*		
UpdateResource	Concede permiso para actualizar los detalles del recurso	Write	organization*		
UpdateSmtpGateway [solo permiso]	Concede permiso para actualizar los detalles de una gateway SMTP existente registrada en una organización	Escritura	organization*		
UpdateUser	Concede permiso para actualizar los detalles de un usuario	Escritura	organization*		
WipeMobileDevice [solo permiso]	Concede permiso para borrar de forma remota el dispositivo móvil asociado a la cuenta de un usuario	Escritura	organization*		

Tipos de recursos definidos por Amazon WorkMail

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
organization	`arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}`	aws:ResourceTag/${TagKey}

Claves de estado de Amazon WorkMail

Amazon WorkMail define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso mediante los pares clave-valor que se pasan en la solicitud.	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por los pares clave-valor de etiqueta adjuntados al recurso	Cadena

Claves de condición	Descripción	Tipo
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon WorkMail Message Flow

Amazon WorkMail Message Flow (prefijo de servicio:`workmailmessageflow`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkMail Message Flow
- Tipos de recursos definidos por Amazon WorkMail Message Flow
- Claves de condición de Amazon WorkMail Message Flow

Acciones definidas por Amazon WorkMail Message Flow

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRawMessageContent	Otorga permiso para leer el contenido de los mensajes de correo electrónico con el ID de mensaje especificado.	Lectura	RawMessage*		
PutRawMessageContent	Otorga permiso para actualizar el contenido de los mensajes de correo electrónico con el ID de mensaje especificado	Escritura	RawMessage*		

Tipos de recursos definidos por Amazon WorkMail Message Flow

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
RawMessage	`arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}`	

Claves de condición de Amazon WorkMail Message Flow

WorkMail Message Flow no tiene claves de contexto específicas de un servicio que puedan usarse como `Condition` elemento de las declaraciones de políticas. Para ver la lista de claves de contexto

globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS global.

Acciones, recursos y claves de condición de Amazon WorkSpaces

Amazon WorkSpaces (prefijo de servicio:`workspaces`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkSpaces
- Tipos de recursos definidos por Amazon WorkSpaces
- Claves de estado de Amazon WorkSpaces

Acciones definidas por Amazon WorkSpaces

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los

que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AcceptAccountLinkInvitation	Otorga permiso para aceptar invitaciones de otras AWS cuentas para compartir la misma configuración de BYOL WorkSpaces	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateConnectionAlias	Otorga permiso para asociar alias de conexión con directorios	Write	connectionalias*		
			directoryid*		
AssociateIpGroups	Otorga permiso para asociar grupos de control de acceso IP a directorios	Escritura	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	Otorga permiso para asociar una aplicación de espacio de trabajo a un WorkSpace	Escritura	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	
AuthorizeIpRules	Otorga permiso para agregar reglas a grupos de control de acceso IP	Escritura	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
CopyWorkspaceImage	Otorga permiso para copiar una WorkSpace imagen	Escritura	workspaceimage*		workspaces:DescribeWorkspaceImages

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountLinkInvitation	Otorga permiso para invitar a otras AWS cuentas a compartir la misma configuración de WorkSpaces BYOL	Escritura			
CreateConnectClientAddIn	Otorga permiso para crear un complemento de cliente de Amazon Connect dentro de un directorio	Escritura	directoryid*		
CreateConnectionAlias	Otorga permiso para crear alias de conexión para su uso con la redirección entre regiones	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIpGroup	Otorga permiso para crear grupos de control de acceso IP	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	
CreateStandbyWorkspaces	Otorga permiso para crear una o más opciones en modo de espera WorkSpaces	Escritura	directoryid*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Otorga permiso para crear etiquetas para WorkSpaces los recursos	Etiquetado		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUpdatedWorkspaceImage	Otorga permiso para crear una WorkSpace imagen actualizada	Escritura	workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceBundle	Otorga permiso para crear un WorkSpace paquete	Escritura	workspacebundle*		workspaces:CreateTags
			workspaceimage*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	Otorga permiso para crear una WorkSpace imagen nueva	Escritura	workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaces	Otorga permiso para crear una o más WorkSpaces	Escritura	directoryid*		
			workspacebundle*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateWorkspacesPool	Otorga permiso para crear un WorkSpaces grupo	Escritura	directoryid*		
			workspacebundle*		
			workspacespoolid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountLinkInvitation	Otorga permiso para eliminar las invitaciones a otras AWS cuentas para que compartan la misma configuración de WorkSpaces BYOL	Escritura			
DeleteClientBranding	Otorga permiso para eliminar los datos de marca del AWS WorkSpaces cliente en un directorio	Escritura	directoryid*		
DeleteConnectClientAddIn	Otorga permiso para eliminar un complemento de cliente de Amazon Connect configurado dentro de un directorio	Escritura	directoryid*		
DeleteConnectionAlias	Otorga permiso para eliminar alias de conexión	Write	connectionalias*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIpGroup	Otorga permiso para eliminar grupos de control de acceso IP	Escritura	workspaceipgroup*		
DeleteTags	Otorga permiso para eliminar etiquetas de WorkSpaces los recursos	Etiquetado		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	Otorga permiso para eliminar WorkSpace paquetes	Escritura	workspacebundle*		
DeleteWorkspaceImage	Otorga permiso para eliminar imágenes WorkSpace	Escritura	workspaceimage*		
DeployWorkspaceApplications	Otorga permiso para implementar todas las aplicaciones de espacio de trabajo pendientes en un WorkSpace	Escritura	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	Otorga permiso para anular el registro de directorios para su uso en Amazon WorkSpaces	Escritura	directoryid*		
DescribeAccount	Otorga permiso para recuperar la configuración de Bring Your Own License (BYOL) para las cuentas WorkSpaces	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeAccountModifications	Otorga permiso para recuperar las modificaciones de la configuración de Bring Your Own License (BYOL) para las cuentas WorkSpaces	Lectura			
DescribeApplicationAssociations	Otorga permiso para recuperar información sobre los recursos asociados a una aplicación WorkSpace	Enumeración	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	Otorga permiso para obtener información sobre WorkSpace las aplicaciones	Enumeración			
DescribeBundleAssociations	Otorga permiso para recuperar información sobre los recursos asociados a un WorkSpace paquete	Enumeración	workspacebundle*		
				aws:ResourceTag/${TagKey}	
DescribeClientBranding	Otorga permiso para recuperar los datos de marca del AWS WorkSpaces cliente en un directorio	Lectura	directoryid*		
DescribeClientProperties	Otorga permiso para recuperar información sobre WorkSpaces los clientes	Enumeración	directoryid*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeConnectClientAddIns	Otorga permiso para obtener una lista de complementos de cliente de Amazon Connect que han sido creados	Enumeración	directoryid*		
DescribeConnectionAliasPermissions	Otorga permiso para recuperar los permisos que los propietarios de los alias de conexión han otorgado a otras AWS cuentas para los alias de conexión	Lectura	connectionalias*		
DescribeConnectionAliases	Otorga permiso para recuperar una lista que describe los alias de conexión utilizados para la redirección entre regiones	Lectura			
DescribeImageAssociations	Otorga permiso para recuperar información sobre los recursos asociados a una imagen WorkSpace	Enumeración	workspaceimage*		
				aws:ResourceTag/${TagKey}	
DescribeIpGroups	Otorga permiso para recuperar información sobre grupos de control de acceso IP	Lectura	workspaceipgroup*		
DescribeTags	Otorga permiso para describir las etiquetas de los WorkSpaces recursos	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeWorkspaceAssociations	Otorga permiso para recuperar información sobre los recursos asociados a un WorkSpace	Enumeración	workspaceid*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	Otorga permiso para obtener información sobre los WorkSpace paquetes	Enumeración			
DescribeWorkspaceDirectories	Otorga permiso para recuperar información sobre los directorios en los que está registrado WorkSpaces	Lectura			
DescribeWorkspaceImagePermissions	Otorga permiso para recuperar información sobre los permisos WorkSpace de imagen	Lectura	workspaceimage*		
DescribeWorkspaceImages	Otorga permiso para recuperar información sobre WorkSpace imágenes	Enumeración			
DescribeWorkspaceSnapshots	Otorga permiso para recuperar información sobre las WorkSpace instantáneas	Enumeración	workspaceid*		
DescribeWorkspaces	Otorga permiso para obtener información sobre WorkSpaces	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DescribeWorkspacesConnectionStatus	Otorga permiso para obtener el estado de conexión de WorkSpaces	Lectura			
DescribeWorkspacesPoolSessions	Otorga permiso para recuperar información sobre las sesiones de un WorkSpaces grupo	Enumeración	workspacespoolid*		
DescribeWorkspacesPools	Otorga permiso para recuperar información sobre los WorkSpaces grupos	Enumeración			
DisassociateConnectionAlias	Otorga permiso para desasociar alias de conexión de directorios	Write	connectionalias*		
DisassociateIpGroups	Otorga permiso para desasociar grupos de control de acceso IP de directorios	Escritura	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	Otorga permiso para desasociar una aplicación de espacio de trabajo de un WorkSpace	Escritura	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetAccountLink	Otorga permiso para recuperar un enlace con otra AWS cuenta para compartir la configuración de BYOL WorkSpaces	Lectura			
ImportClientBranding	Otorga permiso para importar los datos de marca del AWS WorkSpaces cliente a un directorio	Escritura	directoryid*		
ImportWorkspaceImage	Concede permiso para importar imágenes de Bring Your Own License (BYOL) a Amazon WorkSpaces	Escritura			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	Otorga permiso para recuperar los enlaces a las AWS cuentas que comparten tu configuración de BYOL WorkSpaces	Enumeración			
ListAvailableManagementCidrRanges	Otorga permiso para enumerar los rangos de CIDR disponibles para habilitar la licencia Bring Your Own License (BYOL) en las cuentas WorkSpaces	Enumeración			
MigrateWorkspace	Otorga permiso para migrar WorkSpaces	Escritura	workspacebundle*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			workspaceid*		
ModifyAccount	Otorga permiso para modificar la configuración de Bring Your Own License (BYOL) para las cuentas WorkSpaces	Escritura			
ModifyCertificateBasedAuthProperties	Otorga permiso para modificar las propiedades de las autorizaciones basadas en certificados de un directorio	Escritura	directoryid*		
ModifyClientProperties	Otorga permiso para modificar las propiedades de los clientes WorkSpaces	Escritura	directoryid*		
ModifyEndpointEncryptionMode	Otorga permiso para configurar el directorio especificado entre el modo TLS estándar y el modo validado por FIPS 140-2	Escritura	directoryid*		
ModifySamlProperties	Concede permiso para modificar las propiedades SAML de un directorio	Escritura	directoryid*		
ModifySelfservicePermissions	Otorga permiso para modificar las capacidades de WorkSpace administración de autoservicio para sus usuarios	Administración de permisos	directoryid*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ModifyStreamingProperties	Concede permiso para modificar las propiedades de streaming	Escritura	directory id*		
ModifyWorkspaceAccessProperties	Otorga permiso para especificar qué dispositivos y sistemas operativos pueden usar los usuarios para acceder a sus WorkSpaces	Escritura	directory id*		
ModifyWorkspaceCreationProperties	Otorga permiso para modificar las propiedades predeterminadas que se utilizan para crear WorkSpaces	Escritura	directory id*		
ModifyWorkspaceProperties	Otorga permiso para modificar WorkSpace las propiedades, incluidos el modo de ejecución y el AutoStop período	Escritura	workspace id*		
ModifyWorkspaceState	Otorga permiso para modificar el estado de WorkSpaces	Escritura	workspace id*		
RebootWorkspaces	Otorga permiso para reiniciar WorkSpaces	Escritura	workspace id*		
RebuildWorkspaces	Otorga permiso para reconstruir WorkSpaces	Escritura	workspace id*		
RegisterWorkspaceDirectory	Otorga permiso para registrar directorios para su uso con Amazon WorkSpaces	Escritura	directory id*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	Otorga permiso para rechazar invitaciones de otras AWS cuentas para compartir la misma configuración de WorkSpaces BYOL	Escritura			
RestoreWorkspace	Otorga permiso para restaurar WorkSpaces	Escritura	workspaceid*		
RevokeIpRules	Otorga permiso para quitar reglas de grupos de control de acceso IP	Escritura	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
StartWorkspaces	Otorga permiso para comenzar AutoStop WorkSpaces	Escritura	workspaceid*		
StartWorkspacesPool	Otorga permiso para iniciar un WorkSpaces grupo	Escritura	workspacespoolid*		
StopWorkspaces	Otorga permiso para detener AutoStop WorkSpaces	Escritura	workspaceid*		
StopWorkspacesPool	Otorga permiso para detener una WorkSpaces piscina	Escritura	workspacespoolid*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
Stream	Concede permiso a los usuarios federados para iniciar sesión con sus credenciales existentes y transmitir su espacio de trabajo	Escritura	directoryid*		
				workspaces:userId	
TerminateWorkspaces	Otorga permiso para terminar WorkSpaces	Escritura	workspaceid*		
TerminateWorkspacesPool	Otorga permiso para cerrar un WorkSpaces grupo	Escritura	workspacespoolid*		
TerminateWorkspacesPoolSession	Otorga permiso para terminar una sesión de WorkSpaces Pool	Escritura			
UpdateConnectClientAddIn	Otorga permiso para actualizar un complemento de cliente de Amazon Connect. Utilice esta acción para actualizar el nombre y la URL del punto de conexión de un complemento cliente de Amazon Connect	Escritura	directoryid*		
UpdateConnectionAliasPermission	Otorga permiso para compartir o anular el uso compartido de alias de conexión con otras cuentas	Permissions management	connectionalias*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateRulesOfIpGroup	Otorga permiso con el fin de reemplazar reglas para grupos de control de acceso IP	Escritura	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules
UpdateWorkspaceBundle	Otorga permiso para actualizar las WorkSpace imágenes utilizadas en los WorkSpace paquetes	Escritura	workspacebundle*		
			workspaceimage*		
UpdateWorkspaceImagePermission	Otorga permiso para compartir o dejar de compartir WorkSpace imágenes con otras cuentas especificando si otras cuentas tienen permiso para copiar la imagen	Administración de permisos	workspaceimage*		
UpdateWorkspacesPool	Otorga permiso para actualizar el pool WorkSpaces	Escritura	workspacespoolid*		

Tipos de recursos definidos por Amazon WorkSpaces

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
directoryid	arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}	aws:ResourceTag/${TagKey}
workspacebundle	arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}	aws:ResourceTag/${TagKey}
workspaceid	arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
workspaceimage	arn:${Partition}:workspaces:${Region}:${Account}:workspaceimage/${ImageId}	aws:ResourceTag/${TagKey}
workspaceipgroup	arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}	aws:ResourceTag/${TagKey}
workspacespoolid	arn:${Partition}:workspaces:${Region}:${Account}:workspacespool/${PoolId}	aws:ResourceTag/${TagKey}
connectionalias	arn:${Partition}:workspaces:${Region}:${Account}:connectionalias/${ConnectionAliasId}	aws:ResourceTag/${TagKey}
workspaceapplication	arn:${Partition}:workspaces:${Region}:${Account}:workspaceapplication/${WorkSpaceApplicationId}	aws:ResourceTag/${TagKey}

Claves de estado de Amazon WorkSpaces

Amazon WorkSpaces define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulta las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString
workspaces:userId	Filtra el acceso mediante el ID del usuario de WorkSpaces	Cadena

Acciones, recursos y claves de condición de Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager (prefijo de servicio:`wam`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.

- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkSpaces Application Manager
- Tipos de recursos definidos por Amazon WorkSpaces Application Manager
- Claves de condición de Amazon WorkSpaces Application Manager

Acciones definidas por Amazon WorkSpaces Application Manager

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AuthenticatePackager [solo permiso]	Permite que la instancia de empaquetado de Amazon WAM obtenga acceso al catálogo de paquetes de aplicación.	Escritura			

Tipos de recursos definidos por Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager no admite la especificación de un ARN de recurso en el `Resource` elemento de una declaración de política de IAM. Para permitir el acceso a Amazon WorkSpaces Application Manager, `"Resource": "*"` especifíquelo en su política.

Claves de condición de Amazon WorkSpaces Application Manager

WAM no tiene claves de contexto específicas de servicios que se puedan utilizar en el elemento `Condition` de las declaraciones de política. Para ver la lista de las claves de contexto globales que están disponibles para todos los servicios, consulte las claves de contexto de condiciones AWS globales.

Claves de condición, recursos y acciones de las instancias AWS WorkSpaces gestionadas

AWS WorkSpaces Managed Instances (prefijo de servicio:`workspaces-instances`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por las instancias gestionadas AWS WorkSpaces
- Tipos de recursos definidos por las instancias AWS WorkSpaces gestionadas
- Claves de condición para las instancias AWS WorkSpaces administradas

Acciones definidas por las instancias gestionadas AWS WorkSpaces

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla Acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si

la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateVolume	Otorga permiso para asociar un volumen gestionado por un espacio de trabajo a una instancia gestionada por un espacio de trabajo de su cuenta	Escritura	WorkspaceInstanceId*		ec2:AttachVolume ec2:DescribeVolumes
CreateVolume	Otorga permiso para crear un volumen gestionado por	Escritura			ec2:CreateVolume

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
	un espacio de trabajo en tu cuenta				
CreateWorkspaceInstance	Otorga permiso para crear una instancia gestionada por un espacio de trabajo en tu cuenta	Escritura		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:RunInstances
DeleteVolume	Otorga permiso para eliminar un volumen gestionado por un espacio de trabajo en tu cuenta	Escritura	VolumeId*		ec2:DeleteVolume ec2:DescribeVolumes
DeleteWorkspaceInstance	Otorga permiso para eliminar una instancia gestionada por un espacio de trabajo en tu cuenta	Escritura	WorkspaceInstanceId*		ec2:TerminateInstances
DisassociateVolume	Otorga permiso para desasociar un volumen gestionado por un espacio de trabajo de una instancia gestionada por un espacio de trabajo de tu cuenta	Escritura	WorkspaceInstanceId*		ec2:DescribeVolumes ec2:DetachVolume
GetWorkspaceInstance	Otorga permiso para obtener los detalles de una instancia específica gestionada de un espacio de trabajo en tu cuenta	Lectura	WorkspaceInstanceId*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListInstanceTypes	Otorga permiso para enumerar todos los tipos de instancias compatibles	Enumeración			
ListRegions	Otorga permiso para enumerar todas AWS las regiones compatibles	Enumeración			
ListTagsForResource	Otorga permiso para incluir etiquetas de usuario para los recursos de su cuenta	Enumeración	WorkspaceInstanceId*		
ListWorkspaceInstances	Otorga permiso para incluir en tu cuenta las instancias gestionadas por el espacio de trabajo	Enumeración			
TagResource	Otorga permiso para añadir etiquetas de usuario a los recursos de tu cuenta	Etiquetado	WorkspaceInstanceId*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Otorga permiso para eliminar etiquetas de usuario de los recursos de su cuenta	Etiquetado	WorkspaceInstanceId*		
				aws:TagKeys	

Tipos de recursos definidos por las instancias AWS WorkSpaces gestionadas

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
WorkspaceInstanceId	`arn:${Partition}:workspaces-instances:${Region}:${Account}:workspaceinstance/${WorkspaceInstanceId}`	aws:ResourceTag/${TagKey}
VolumeId	`arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}`	aws:ResourceTag/${TagKey}

Claves de condición para las instancias AWS WorkSpaces administradas

AWS WorkSpaces Managed Instances define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra acciones basadas en las etiquetas que se aprueban en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra acciones en función de la etiqueta asociada con el recurso	Cadena
aws:TagKeys	Filtra acciones basadas en las claves de etiqueta que se aprueban en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser (prefijo de servicio:`workspaces-web`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkSpaces Secure Browser
- Tipos de recursos definidos por Amazon WorkSpaces Secure Browser
- Claves de condición de Amazon WorkSpaces Secure Browser

Acciones definidas por Amazon WorkSpaces Secure Browser

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla

el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
AssociateBrowserSettings	Concede permiso para asociar la configuración del navegador a portales web	Escritura	browserSettings*		
			portal*		
AssociateDataProtectionSettings	Otorga permiso para asociar la configuración de protección de datos a los portales web	Escritura	dataProtectionSettings*		
			portal*		
AssociateIpAccessSettings	Concede permiso para asociar la configuración de acceso de IP con portales web	Escritura	ipAccessSettings*		
			portal*		
AssociateNetworkSettings	Concede permiso para asociar la configuración de red a portales web	Escritura	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkI

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					nterfaceP ermission ec2:Modif yNetworkI nterfaceA ttribute
			portal*		
Associate TrustStore	Concede permiso para asociar tiendas de confianza a portales web	Escritura	portal*		
			trustStor e*		
Associate UserAcces sLoggingS ettings	Concede permiso para asociar la configuración del registro del acceso de los usuarios con portales web	Escritura	portal*		kinesis:P utRecord kinesis:P utRecords
			userAcces sLoggingS ettings*		
Associate UserSettings	Concede permiso para asociar la configuración de usuario con portales web	Escritura	portal*		
			userSetti ngs*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateBrowserSettings	Concede permiso para crear configuración de navegador	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
CreateDataProtectionSettings	Otorga permiso para crear ajustes de protección de datos	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateIdentityProvider	Concede permiso para crear proveedores de identidades	Escritura	identityProvider* portal*	aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateIpAccessSettings	Concede permiso para crear la configuración de acceso de IP	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetworkSettings	Concede permiso para crear configuración de redes	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreatePortal	Concede permiso para crear portales web	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateTrustStore	Concede permiso para crear tiendas de confianza	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateUserAccessLoggingSettings	Concede permiso para crear la configuración del registro del acceso de los usuarios	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
CreateUserSettings	Concede permiso para crear configuración de usuario.	Escritura		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBrowserSettings	Concede permiso para eliminar la configuración del navegador	Escritura	browserSettings*		
DeleteDataProtectionSettings	Otorga permiso para eliminar la configuración de protección de datos	Escritura	dataProtectionSettings*		
DeleteIdentityProvider	Concede permiso para eliminar proveedores de identidad	Escritura	identityProvider* portal*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteIpAccessSettings	Concede permiso para eliminar la configuración de acceso de IP	Escritura	ipAccessSettings*		
DeleteNetworkSettings	Concede permiso para eliminar configuración de red	Escritura	networkSettings*		
DeletePortal	Concede permiso para eliminar portales web	Escritura	portal*		
DeleteTrustStore	Concede permiso para eliminar tiendas de confianza	Escritura	trustStore*		
DeleteUserAccessLoggingSettings	Concede permiso para eliminar la configuración del registro del acceso de los usuarios	Escritura	userAccessLoggingSettings*		
DeleteUserSettings	Concede permiso para eliminar configuración de usuario	Escritura	userSettings*		
DisassociateBrowserSettings	Concede permiso para disociar la configuración del navegador de los portales web	Escritura	portal*		
DisassociateDataProtectionSettings	Otorga permiso para desasociar los registros de protección de datos de los portales web	Escritura	portal*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DisassociateIpAccessSettings	Concede permiso para desasociar el registro de la configuración de acceso de IP de portales web	Escritura	portal*		
DisassociateNetworkSettings	Concede permiso para disociar la configuración de red de los portales web	Escritura	portal*		
DisassociateTrustStore	Concede permiso para desasociar tiendas de confianza de los portales web	Escritura	portal*		
DisassociateUserAccessLoggingSettings	Concede permiso para desasociar la configuración del registro del acceso de los usuarios de los portales web	Escritura	portal*		
DisassociateUserSettings	Concede permiso para desasociar la configuración de usuario de los portales web	Escritura	portal*		
ExpireSession	Concede permiso para caducar una sesión de un portal específico	Escritura	portal*		
GetBrowserSettings	Concede permiso para obtener detalles acerca de la configuración del navegador	Lectura	browserSettings*		
GetDataProtectionSettings	Otorga permiso para obtener detalles sobre la configuración de protección de datos	Lectura	dataProtectionSettings*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIdentityProvider	Concede permiso para obtener detalles acerca de los proveedores de identidad	Lectura	identityProvider*		
GetIpAccessSettings	Concede permiso para obtener detalles sobre la configuración de acceso de IP	Lectura	ipAccessSettings*		
GetNetworkSettings	Concede permiso para obtener detalles acerca de la configuración de red	Lectura	networkSettings*		
GetPortal	Concede permiso para obtener detalles acerca de los portales web	Lectura	portal*		
GetPortalServiceProviderMetadata	Concede permiso para obtener información de metadatos del proveedor de servicios para portales web	Lectura	portal*		
GetSession	Concede permiso para obtener información sobre una sesión particular para un portal	Lectura	portal*		
GetTrustStore	Concede permiso para obtener detalles acerca de tiendas de confianza	Lectura	trustStore*		
GetTrustStoreCertificate	Concede permiso para obtener certificados de tiendas de confianza	Lectura	trustStore*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetUserAccessLoggingSettings	Concede permiso para obtener detalles acerca de la configuración del registro del acceso de los usuarios	Lectura	userAccessLoggingSettings*		
GetUserSettings	Concede permiso para obtener detalles acerca de la configuración del usuario	Lectura	userSettings*		
ListBrowserSettings	Concede permiso para enumerar la configuración del navegador	Lectura			
ListDataProtectionSettings	Otorga permiso para enumerar las configuraciones de protección de datos	Lectura			
ListIdentityProviders	Concede permiso para enumerar los proveedores de identidad	Lectura	identityProvider*		
ListIpAccessSettings	Concede permiso para enumerar la configuración de acceso de IP	Lectura			
ListNetworkSettings	Concede permiso para enumerar la configuración de red	Lectura			
ListPortals	Concede permiso para enumerar los portales web	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListSessions	Concede permiso para enumerar las sesiones para un portal con filtros opcionales	Lectura	portal*		
ListTagsForResource	Concede permiso para enumerar las etiquetas de un recurso	Lectura			
ListTrustStoreCertificates	Concede permiso para enumerar certificados en una tienda de confianza	Lectura			
ListTrustStores	Concede permiso para enumerar tiendas de confianza	Lectura			
ListUserAccessLoggingSettings	Concede permiso para enumerar la configuración del registro del acceso de los usuarios	Lectura			
ListUserSettings	Concede permiso para enumerar la configuración de usuario	Lectura			
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso	Etiquetado	browserSettings		
			dataProtectionSettings		
			identityProvider		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ipAccessSettings		
			networkSettings		
			portal		
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	browserSettings		
			dataProtectionSettings		
			identityProvider		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			ipAccessSettings		
			networkSettings		
			portal		
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys	
UpdateBrowserSettings	Concede permiso para actualizar una configuración de navegador	Escritura	browserSettings*		
UpdateDataProtectionSettings	Otorga permiso para actualizar la configuración de protección de datos	Escritura	dataProtectionSettings*		
UpdateIdentityProvider	Concede permiso para actualizar un proveedor de identidades	Escritura	identityProvider*		
			portal*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateIpAccessSettings	Concede permiso para actualizar la configuración de acceso de IP	Escritura	ipAccessSettings*		
UpdateNetworkSettings	Concede permiso para actualizar una configuración de red	Escritura	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
UpdatePortal	Concede permiso para actualizar portales web	Escritura	portal*		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UpdateTrustStore	Concede permiso para actualizar tiendas de confianza	Escritura	trustStore*		
UpdateUserAccessLoggingSettings	Concede permiso para actualizar la configuración del registro del acceso de los usuarios	Escritura	userAccessLoggingSettings*		kinesis:PutRecord kinesis:PutRecords
UpdateUserSettings	Concede permiso para actualizar una configuración de usuario.	Escritura	userSettings*		

Tipos de recursos definidos por Amazon WorkSpaces Secure Browser

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
browserSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:browserSettings/${BrowserSettingsId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
identityProvider	arn:${Partition}:workspaces-web:${Region}:${Account}:identityProvider/${PortalId}/${IdentityProviderId}	aws:ResourceTag/${TagKey}
networkSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:networkSettings/${NetworkSettingsId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:workspaces-web:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
trustStore	arn:${Partition}:workspaces-web:${Region}:${Account}:trustStore/${TrustStoreId}	aws:ResourceTag/${TagKey}
userSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userSettings/${UserSettingsId}	aws:ResourceTag/${TagKey}
userAccessLoggingSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userAccessLoggingSettings/${UserAccessLoggingSettingsId}	aws:ResourceTag/${TagKey}
ipAccessSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:ipAccessSettings/${IpAccessSettingsId}	aws:ResourceTag/${TagKey}
dataProtectionSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:dataProtectionSettings/${DataProtectionSettingsId}	aws:ResourceTag/${TagKey}

Claves de condición de Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Claves de condición, recursos y acciones de Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client (prefijo de servicio:`thinclient`) proporciona los siguientes recursos, acciones y claves de contexto de condición específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por Amazon WorkSpaces Thin Client
- Tipos de recursos definidos por Amazon WorkSpaces Thin Client
- Claves de condición de Amazon WorkSpaces Thin Client

Acciones definidas por Amazon WorkSpaces Thin Client

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, administración de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CreateEnvironment	Concede permiso para crear entornos	Escritura		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	appstream:DescribeStacks iam:CreateServiceLinkedRole workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:Describ

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
					eWorkspaceDirectories
DeleteDevice	Concede permiso para eliminar dispositivos	Escritura	device*		
				aws:ResourceTag/${TagKey}	
DeleteEnvironment	Concede permiso para eliminar entornos	Escritura	environment*		
				aws:ResourceTag/${TagKey}	
DeregisterDevice	Concede permiso para anular el registro de dispositivos	Escritura	device*		
				aws:ResourceTag/${TagKey}	
GetDevice	Otorga permiso para obtener dispositivos	Lectura	device*		
				aws:ResourceTag/${TagKey}	
GetDeviceDetails [solo permiso]	Concede permiso para obtener detalles de dispositivos	Lectura	device*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetEnvironment	Concede permiso para obtener detalles de entornos	Lectura	environment*		
				aws:ResourceTag/${TagKey}	
GetSoftwareSet	Concede permiso para obtener detalles de conjuntos de software	Lectura	softwareset*		
				aws:ResourceTag/${TagKey}	
ListDeviceSessions [solo permiso]	Concede permiso para enumerar sesiones de dispositivos	Enumeración	device*		
				aws:ResourceTag/${TagKey}	
ListDevices	Concede permiso para enumerar dispositivos	Enumeración			
ListEnvironments	Otorga permiso para enumerar los entornos.	Enumeración			
ListSoftwareSets	Concede permiso para enumerar conjuntos de software	Enumeración			
ListTagsForResource	Concede permiso para obtener una lista de etiquetas para un recurso.	Enumeración	device		
			environment		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
			softwareset		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permiso para agregar una o varias etiquetas a un recurso	Etiquetado	device		
			environment		
			softwareset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permiso para eliminar una o varias etiquetas de un recurso.	Etiquetado	device		
			environment		
			softwareset		

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateDevice	Concede permiso para actualizar dispositivos	Escritura	device*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	Otorga permiso para actualizar entornos	Escritura	environment*		appstream:DescribeStacks workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
				aws:ResourceTag/${TagKey}	
UpdateSoftwareSet	Concede permiso para actualizar un conjunto de software	Escritura	softwareset*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos por Amazon WorkSpaces Thin Client

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
environment	`arn:${Partition}:thinclient:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:thinclient:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}

Tipos de recurso	ARN	Claves de condición
softwareset	`arn:${Partition}:thinclient:${Region}:${Account}:softwareset/${SoftwareSetId}`	aws:ResourceTag/${TagKey}

Claves de condición de Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Acciones, recursos y claves de condición para AWS X-Ray

AWS X-Ray (prefijo de servicio:`xray`) proporciona los siguientes recursos, acciones y claves de contexto de condiciones específicos del servicio para su uso en las políticas de permisos de IAM.

Referencias:

- Obtenga información para configurar este servicio.
- Vea una lista de las operaciones de API disponibles para este servicio.
- Obtenga información sobre cómo proteger este servicio y sus recursos mediante las políticas de permisos de IAM.

Temas

- Acciones definidas por AWS X-Ray
- Tipos de recursos definidos por AWS X-Ray
- Claves de condición para AWS X-Ray

Acciones definidas por AWS X-Ray

Puede especificar las siguientes acciones en el elemento `Action` de una declaración de política de IAM. Utilice políticas para conceder permisos para realizar una operación en AWS. Cuando utiliza una acción en una política, normalmente permite o deniega el acceso a la operación de la API o comandos de la CLI con el mismo nombre. No obstante, en algunos casos, una sola acción controla el acceso a más de una operación. Asimismo, algunas operaciones requieren varias acciones diferentes.

La columna Nivel de acceso de la tabla de acciones describe cómo se clasifica la acción (lista, lectura, gestión de permisos o etiquetado). Esta clasificación puede ayudarle a entender el nivel de acceso que una acción concede cuando se utiliza en una política. Para obtener más información sobre los niveles de acceso, consulte los niveles de acceso en los resúmenes de políticas.

La columna Tipos de recurso de la tabla de Acción indica si cada acción admite permisos de nivel de recursos. Si no hay ningún valor para esta columna, debe especificar todos los recursos ("*") a los que aplica la política en el elemento `Resource` de la instrucción de su política. Si la columna incluye un tipo de recurso, puede especificar un ARN de ese tipo en una instrucción con dicha acción. Si la acción tiene uno o más recursos necesarios, la persona que llama debe tener permiso para usar la acción con esos recursos. Los recursos necesarios se indican en la tabla con un asterisco (*). Si limita el acceso a los recursos con el elemento `Resource` de una política de IAM, debe incluir un ARN o patrón para cada tipo de recurso requerido. Algunas acciones admiten varios tipos de recursos. Si el tipo de recurso es opcional (no se indica como obligatorio), puede elegir utilizar uno de los tipos de recursos opcionales.

La columna Claves de condición de la tabla Acciones incluye claves que puede especificar en el elemento `Condition` de la instrucción de una política. Para obtener más información sobre las claves de condición asociadas a los recursos del servicio, consulte la columna Claves de condición de la tabla Tipos de recursos.

> **Note**
>
> Las claves de condición de recursos se enumeran en la tabla Tipos de recursos. Encontrará un enlace al tipo de recurso que se aplica a una acción en la columna Tipos de recursos (*obligatorio) de la tabla Acciones. El tipo de recurso de la tabla Tipos de recursos incluye la columna Claves de condición, que son las claves de condición del recurso que se aplican a una acción de la tabla Acciones.

Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Acciones.

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
BatchGetTraceSummaryById [solo permiso]	Otorga permiso para recuperar metadatos de una lista de rastros especificados por ID	Lectura			
BatchGetTraces	Otorga permiso para recuperar una lista de trazas especificadas por ID. Cada rastro es una recopilación de documentos de segmentos procedente de una única solicitud. Úselo GetTraceSummaries para obtener una lista de trazas IDs	Enumeración			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
CancelTraceRetrieval	Concede permiso para cancelar un trabajo de recuperación de trazas en curso iniciado StartTraceRetrieval con los datos proporcionados Retrieval Token. Una cancelación correcta devolverá una respuesta HTTP 200	Lectura			
CreateGroup	Otorga permiso para crear un recurso de grupo con un nombre y una expresión de filtro	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSamplingRule	Otorga permiso para crear una regla para controlar el comportamiento de muestreo para aplicaciones instrumentadas	Write	sampling-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	Otorga permiso para eliminar una política de recursos.	Escritura	group*		
				aws:ResourceTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
DeleteResourcePolicy	Otorga permiso para eliminar políticas de recursos	Escritura			
DeleteSamplingRule	Otorga permiso para eliminar una regla de muestreo	Escritura	sampling-rule*		
				aws:ResourceTag/${TagKey}	
GetDistinctTraceGraphs [solo permiso]	Otorga permiso para recuperar gráficos de servicio distintos para uno o más rastreos específicos IDs	Lectura			
GetEncryptionConfig	Otorga permiso para recuperar la configuración de cifrado actual para los datos de X-Ray	Read			
GetGroup	Otorga permiso para recuperar detalles de recursos de grupo	Read	group*		
				aws:ResourceTag/${TagKey}	
GetGroups	Otorga permiso para recuperar todos los detalles del grupo activo	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetIndexingRules	Otorga permiso para recuperar todas las reglas de indexación. Las reglas de indexación se utilizan para determinar la frecuencia de muestreo del lado del servidor para los intervalos ingeridos a través del CloudWatchLogs destino e indexados por X-Ray	Lectura			
GetInsight	Otorga permiso para recuperar los detalles de una información específica	Read			
GetInsightEvents	Otorga permiso para recuperar los eventos de una visión específica	Read			
GetInsightImpactGraph	Otorga permiso para recuperar la parte del gráfico de servicio que se ve afectada para obtener una información específica	Read			
GetInsightSummaries	Otorga permiso para recuperar el resumen de todas las perspectivas de un grupo y un intervalo de tiempo con filtros opcionales	Lectura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetRetrievedTracesGraph	Otorga permiso para recuperar un gráfico de servicio para los rastreos en función de lo especificado RetrievalToken en el grupo de registros de búsqueda de transacciones CloudWatch	Lectura			
GetSamplingRules	Otorga permiso para recuperar todas las reglas de muestreo	Read			
GetSamplingStatisticSummaries	Otorga permiso para recuperar información sobre los resultados de muestreo recientes para todas las reglas de muestreo	Read			
GetSamplingTargets	Otorga permiso para solicitar una cuota de muestreo para las reglas que el servicio está utilizando para muestrear solicitudes	Read			
GetServiceGraph	Recupera un documento que describe los servicios que procesan solicitudes entrantes y los servicios posteriores a los que llaman como resultado .	Read			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
GetTimeSeriesServiceStatistics	Obtenga permiso para recuperar una agregación de estadísticas de servicio definida mediante un intervalo de tiempo específico integrado en buckets en intervalos de tiempo	Lectura			
GetTraceGraph	Otorga permiso para recuperar un gráfico de servicio para uno o más rastreos específicos IDs	Lectura			
GetTraceSegmentDestination	Otorga permiso para recuperar el destino actual de los datos enviados a PutTraceSegments una OpenTelemetry API	Lectura			
GetTraceSummaries	Otorga permiso para recuperar IDs los metadatos de los rastreos disponibles durante un período de tiempo específico mediante un filtro opcional. Para obtener los rastreos completos, pase el rastreo IDs a BatchGetTraces	Lectura			
Link [solo permiso]	Otorga permiso para compartir recursos de X-Ray con una cuenta de monitoreo	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
ListResourcePolicies	Otorga permiso para enumerar las políticas de recursos	Enumeración			
ListRetrievedTraces	Otorga permiso para recuperar una lista de rastreos de una determinada información RetrievalToken del grupo de CloudWatch registros de búsqueda de transacciones	Enumeración			
ListTagsForResource	Otorga permiso para obtener una lista de etiquetas para un recurso de X-Ray	List	group		
			sampling-rule		
PutEncryptionConfig	Otorga permiso para actualizar la configuración de cifrado de datos de X-Ray	Administración de permisos			
PutResourcePolicy	Otorga permiso para crear o actualizar políticas de recursos	Escritura			
PutSpans	Otorga permiso para subir OpenTelemetry tramos a X-Ray AWS	Escritura			
PutSpansForIndexing [solo permiso]	Otorga permiso para subir tramos a AWS X-Ray para indexarlos	Escritura			

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
PutTelemetryRecords	Otorga permiso para enviar la telemetría del daemon de AWS X-Ray al servicio	Escritura			
PutTraceSegments	Otorga permiso para cargar documentos segmentados en AWS X-Ray. El SDK de X-Ray genera documentos de segmentos y los envía al daemon de X-Ray, que lo carga en lotes.	Escritura			
StartTraceRetrieval	Otorga permiso para iniciar un proceso de recuperación de trazas en el intervalo de tiempo especificado y para el rastreo dado en cuestión IDs en el grupo de CloudWatch registros de búsqueda de transacciones	Lectura			
TagResource	Otorga permiso para agregar etiquetas a un recurso de X-Ray	Etiquetado	group		
			sampling-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	

Acciones	Descripción	Nivel de acceso	Tipos de recursos (*necesarios)	Claves de condición	Acciones dependientes
UntagResource	Otorga permiso para eliminar etiquetas de un recurso de X-Ray	Etiquetado	group		
			sampling-rule		
				aws:TagKeys	
UpdateGroup	Otorga permiso para actualizar un recurso de grupo.	Escritura	group*		
				aws:ResourceTag/${TagKey}	
UpdateIndexingRule	Otorga permiso para modificar la configuración de una regla de indexación	Escritura			
UpdateSamplingRule	Otorga permiso para modificar la configuración de una regla de muestreo	Escritura	sampling-rule*		
				aws:ResourceTag/${TagKey}	
UpdateTraceSegmentDestination	Otorga permiso para modificar el destino de los datos enviados a una PutTraceSegments API OpenTelemetry	Escritura			

Tipos de recursos definidos por AWS X-Ray

Los siguientes tipos de recurso están definidos por este servicio y se pueden utilizar en el elemento `Resource` de las instrucciones de política de permisos de IAM. Cada acción de la tabla Acciones identifica los tipos de recursos que se pueden especificar con dicha acción. Un tipo de recurso también puede definir qué claves de condición se pueden incluir en una política. Estas claves se muestran en la última columna de la tabla Tipos de recursos. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla Tipos de recurso.

Tipos de recurso	ARN	Claves de condición
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	aws:ResourceTag/${TagKey}
sampling-rule	`arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}`	aws:ResourceTag/${TagKey}

Claves de condición para AWS X-Ray

AWS X-Ray define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener información detallada sobre las columnas de la siguiente tabla, consulte Tabla de Claves de condición.

Para ver las claves de condición globales que están disponibles para todos los servicios, consulte las claves de contexto de condición AWS globales.

Claves de condición	Descripción	Tipo
aws:RequestTag/${TagKey}	Filtra el acceso por las etiquetas que se pasan en la solicitud	Cadena

Claves de condición	Descripción	Tipo
aws:ResourceTag/${TagKey}	Filtra el acceso por las etiquetas asociadas al recurso	Cadena
aws:TagKeys	Filtra el acceso por las claves de etiquetas que se pasan en la solicitud	ArrayOfString

Recursos relacionados

Para obtener información relacionada en la Guía del usuario de IAM, consulte los siguientes recursos:

- Tutorial: Crear y asociar su primera política administrada por el cliente
- AWS servicios que funcionan con IAM
- Lógica de evaluación de políticas

Servicio de AWS Información simplificada para acceso programático

AWS proporciona información de referencia del servicio en formato JSON para agilizar la automatización de los flujos de trabajo de gestión de políticas. Con la información de referencia del servicio, puede acceder a las acciones, los recursos y las claves de condición disponibles Servicios de AWS desde archivos legibles por máquina. Los administradores de seguridad pueden establecer barreras y los desarrolladores pueden garantizar el acceso adecuado a las aplicaciones identificando las acciones, los recursos y las claves de condición disponibles para cada una de ellas. Servicio de AWS AWS proporciona información de referencia sobre el servicio Servicios de AWS para que pueda incorporar los metadatos en sus flujos de trabajo de administración de políticas.

Para obtener un inventario de las acciones, los recursos y las claves de condición que se utilizarán en las políticas de IAM, consulte la página de referencia sobre la autorización de servicios para el Servicio de AWS.

Las acciones, los recursos y las claves de condición de los servicios que comparten un prefijo de servicio pueden dividirse en varias páginas en la Referencia de autorización de servicio.

El contenido presentado en la Referencia de autorización de servicio puede presentarse de forma diferente o contener metadatos diferentes. Para obtener más información, consulte Definiciones de campos adicionales.

> **Note**
>
> Los cambios en la información de referencia del servicio pueden tardar hasta 24 horas en reflejarse en la lista de metadatos del servicio.

Acceder a Servicio de AWS la información de referencia

1. Navegue hasta la información de referencia del servicio para acceder a la lista de Servicios de AWS la que está disponible la información de referencia.

   El siguiente ejemplo muestra una lista parcial de los servicios y URLs su información de referencia correspondiente:

   ```
   [
   ```

```
    {
        "service": "s3",
        "url": "https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json"
    },
    {
        "service": "dynamodb",
        "url": "https://servicereference.us-east-1.amazonaws.com/v1/dynamodb/
dynamodb.json"
    },
    …
]
```

2. Elija un servicio y navegue hasta la página de información del servicio en el `url` campo correspondiente para ver una lista de acciones, recursos y claves de condición del servicio.

   El siguiente ejemplo muestra una lista parcial de información de referencia de servicios para Amazon S3:

```
{
    "Name": "s3",
    "Actions": [
        {
            "Name": "GetObject",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : false,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
```

```
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "object"
                }
            ]
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : true,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "bucket"
                }
            ]
        },
        ...
    ],
    "ConditionKeys": [
        {
```

```
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.2"
}
```


3. Descargue el archivo JSON de la URL del servicio para utilizarlo en los flujos de trabajo de creación de políticas.

Definiciones de campos adicionales

Las propiedades de las acciones proporcionan metadatos adicionales sobre las acciones del servicio para ayudar a clasificarlas en función del ámbito de sus permisos. Estas propiedades se encuentran en el `Annotations` campo de cada acción. Los metadatos se componen de cuatro valores booleanos:

- `IsList`— Proporciona permisos para descubrir y enumerar recursos, incluidos los metadatos básicos, sin acceder al contenido de los recursos.

  Ejemplo: esta propiedad corresponde a la `ListBucket` acción `true` de Amazon S3, que permite a los usuarios ver las listas de buckets sin tener que acceder ellos mismos a los objetos.
- `IsPermissionManagement`— Proporciona permisos para modificar los permisos de IAM o las credenciales de acceso.

  Ejemplo: esta propiedad es `true` para la mayoría de las AWS Organizations acciones y de IAM, así como para las acciones de Amazon S3, como `PutBucketPolicy` y`DeleteBucketPolicy`.
- `IsTaggingOnly`— Proporciona permisos únicamente para modificar etiquetas.

  Ejemplo: esta propiedad es `true` para acciones de IAM `TagRole` y`UntagRole`, si bien está `false` destinada, proporciona permisos más `CreateRole` amplios que van más allá del etiquetado.
- `IsWrite`— Proporciona permisos para modificar los recursos, lo que puede incluir modificaciones en las etiquetas.

  Ejemplo: esta propiedad es `true` para las acciones `CreateBucket` de Amazon S3 y `PutObject` porque permiten la modificación de recursos. `DeleteBucket`

> **Note**
>
> Estas propiedades no se excluyen mutuamente. Una acción puede tener varias propiedades configuradas en`true`.
> También es posible que todas las propiedades lo sean`false`, como se ve en la `GetObject` acción de Amazon S3. Esto indica que la acción solo otorga permisos de lectura sobre un objeto.

Estas propiedades se pueden utilizar para generar información sobre los servicios. El siguiente ejemplo muestra qué permisos con el `s3` prefijo permiten mutar los recursos:

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsWrite == true) | .Name'

"AssociateAccessGrantsIdentityCenter"
"BypassGovernanceRetention"
```

```
"CreateAccessGrant"
"CreateAccessGrantsInstance"
"CreateAccessGrantsLocation"
...
```

En el siguiente ejemplo, se muestran las claves de condición de acción con el `lambda` prefijo que puede utilizar para limitar el acceso a las acciones de administración de permisos:

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/lambda/lambda.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsPermissionManagement == true) |
 {Name: .Name, ActionConditionKeys: (.ActionConditionKeys // [])}'

{
   "Name": "AddLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "AddPermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
{
    "Name": "DisableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "EnableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "RemoveLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "RemovePermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
```

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.